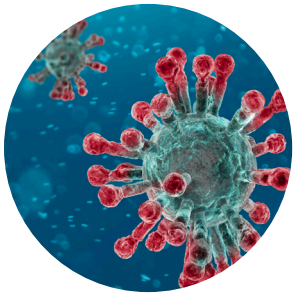
NORCAL GROUP®

TELEMEDICINE AND COMMUNICATIONS
RESOURCE BUNDLE FOR COVID-19 PANDEMIC RESPONSE



While COVID-19 may require adjustments to how you provide care, certain principles - including standard of care and compliance with federal, state and local regulations - still need to be reinforced. The attached NORCAL Group Risk Management resources contain strategies for assuring appropriate and compliant communication with patients. We hope that this packet of information will offer you guidance as you navigate these challenges to care provision.

Our Risk Management team is committed to assisting you:

Monday-Friday from 8am – 8pm ET **855.882.3412** **risksolutions@norcal-group.com**

ABOUT NORCAL GROUP

The NORCAL Group of companies provide medical professional liability insurance, risk management solutions and provider wellness resources to physicians, healthcare extenders, medical groups, hospitals, community clinics, and allied healthcare facilities throughout the country. NORCAL Group includes NORCAL Mutual Insurance Company and its affiliated insurance companies. Please visit norcal-group.com/companies for more information.

NORCAL GROUP®

TABLE OF CONTENTS

Contents of this packet include the following resources and associated sample forms:

NORCAL GROUP®

RISK MANAGEMENT RESOURCE

TELEMEDICINE RECOMMENDATIONS

TELEMEDICINE

Many practices are investigating the use of telemedicine to offer services while minimizing risks to their patients and staff. For those practices that have not established telemedicine, there are several key elements that should be considered. Telehealth and telemedicine may be defined by state laws and regulations, but the specificity may vary widely. In addition, compensation for providing telemedicine services will also depend upon the patient's insurance provider, therefore impacting reimbursement. In addition, the use of technology to communicate with and evaluate patients requires attention to privacy and security practices as well as assuring the standard of care is met.

Risk Management Recommendations

As more and more healthcare providers begin to use telehealth to care for their patients, it is important to always remain mindful of general patient safety, the individuals' clinical care needs, and what would always be your fundamental guiding light—the standard of care for your clinical decisions. That means applying your best judgment, reasonable care and diligence under the current circumstances. Some situations may be extreme, e.g., COVID-19, with limited resource allocation and human exhaustion. Again, the standard of care in this context is best judgment and reasonable care within that particular situation. Documentation of specific, relevant factors and rationale are very important. Utilize all the risk mitigating and patient safety tools you would normally use—that of thorough communication, coordination of care, and documentation of both, as well as your clinical thinking and decision-making process.

- Ensure the patient's condition can be appropriately examined via available telehealth equipment. Determination of telehealth appropriateness will need to be made, e.g., can the patient be adequately assessed without information normally obtained during an office visit.
- Ensure the patient has the technology and connectivity necessary to be adequately examined and the capability to utilize the technology needed.
- Ensure that you are examining and prescribing for the correct patient. Some ways to authenticate the patient include:
  - Asking the patient to hold up a driver's license to the camera and comparing the information on the identification card to the information provided by the patient.
  - Running an insurance eligibility check, confirming the patient's name, address, date of birth and Social Security number.
  - If the patient has been seen before, asking a series of questions on prior medical history to determine if the patient responses match what is in the medical records.
- Thoroughly document the encounter as you would any face-to-face encounter, including all communications with or about the patient, review or ordering of tests / results and follow-up recommendations, coordination of care, etc.
- Document the informed consent process and confirmation, including that the patient agrees to and understands the limits of confidentiality when communicating via an electronic medium and that it may be determined that telemedicine is not appropriate for the diagnosis and treatment of his or her condition.
- Document any technical issues that interfered with, delayed or complicated the telemedicine encounter. For example, poor internet connectivity or signal quality, camera or device malfunction, tele-presenter unavailability, patient inability to manage technical aspects of the exam, or peripheral device unavailability.

National Resources

- The Center for Connected Health Policy's (CCHP) National Telehealth Policy and Resource Center (NTRC-P) is a nonprofit, nonpartisan organization working to maximize telehealth's ability to improve health outcomes, care delivery and cost effectiveness. One of the most inclusive resources; it is a very robust and easy to use website. Lists 50-state laws, reimbursement regulations, policies, resources and multiple links (as well as telephone contacts) for detailed resources and information. Located: https://www.cchpca.org/. Must join but membership is free.
- As many practices are rapidly implementing telemedicine services, interstate licensure has become increasingly important. Many states have enacted regulations waiving state licensure requirements for healthcare providers through Emergency Declarations. The Federation of State Medical Boards has compiled a PDF list of states that have waived licensure requirements with links to each state's relevant information. https://www.fsmb.org/advocacy/covid-19/
- The Office for Civil Rights, U.S. Department of Health and Human Services issued a bulletin in response to the COVID-19 virus to address how patient information may be shared under the HIPAA Privacy Rule in an outbreak of infectious disease and to remind covered entities and their business associates that the protections of the Privacy Rule are still in force during an emergency. https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html
- The National Consortium of Telehealth Resource Centers (NCTRC) is funded by the U.S. Department of Health and Human Services (HHS) Health Resources and Services Administration (HRSA). Telehealth Resource Centers (TRCs) located throughout the United States work collaboratively to provide information and assistance to telehealth providers. https://www.telehealthresourcecenter.org/
- The Center for Medicare and Medicaid Services (CMS) has issued information and guidance on telehealth related to the President's Emergency Declaration.
  - https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet
  - https://www.cms.gov/newsroom/press-releases/president-trump-expands-telehealth-benefits-medicare-beneficiaries-during-covid-19-outbreak

For additional Telemedicine and Specialty Specific Resources, please visit our *Telemedicine Resource page*.

NORCAL GROUP®

RISK MANAGEMENT RESOURCE

CREATIVE AND PRACTICAL COVID-19 TELEHEALTH CONSENT STRATEGIES

NORCAL GROUP®

CREATIVE AND PRACTICAL COVID-19 TELEHEALTH CONSENT STRATEGIES

How to document consent for telemedicine if traditional use of a form is not feasible

PATIENT PORTAL

› Ask your vendor to include the contents of your telehealth consent form as an online form with a digital acceptance and signature.

EMAIL

› Email the fillable Telehealth Consent Form (PDF). Use "request a read receipt" if possible.
- The patient can sign digitally and email it back to you.
- They can review it ahead of the call and give their consent by phone, text or email. Document your method and rationale in the chart.

VIDEO ENCOUNTER

› If conducting video telemedicine, show the consent at the beginning of the encounter and review the contents.
- Document your method and rationale in the chart.

TEXT

› Take a picture of the form with your phone and text it to the patient ahead of the call and have them text back their agreement.
- Document your method and rationale in the chart. Include screenshot or text in your chart if possible.

› Text the form as above and review the elements at the beginning of their telemedicine encounter.
- Document your method and rationale in the chart.

PHONE ONLY

› If providing services through audio contact only where email and texting are not options, discuss the elements of the consent.
- Document your method and rationale in the chart.

Attempt to obtain a written consent at a future date, if possible, to support your documentation. Documentation should include the rationale for using these alternative communication strategies. When written consent is not possible, please see the following recommendations.

Obtaining Consent Over the Phone

There may be situations where it is not possible to send and receive back a signed Telemedicine consent prior to a visit. In an effort to ensure access to medical care during the COVID-19 Pandemic, providers may need to obtain consent over the phone. In these situations, it is important to document the steps you took to obtain consent in this manner and your documentation should include:

- Verification of the authenticity of the patient by requesting their full name, date of birth, address, and phone number(s) and any other verifiable means (e.g., their medical history)
- That you explained the definition of Telemedicine and why it was being used for this visit during the COVID-19 Pandemic.

  Defining Telemedicine: Telemedicine and telehealth are often used interchangeably. They both refer to the use of technology to deliver healthcare at a distance including any type of patient care that involves telecommunication. You may wish to include mention of any of these modes that may apply to your visits; such as videoconferencing, transmission of still images and other data, e-health (patient portals, websites), m-health (mobile healthcare service), remote monitoring and medical call centers.

(See Claims Rx: February 2018 in our Telemedicine and Communications Resource Bundle.)

- Discussion of the risks, benefits, and alternatives with the patient. Be sure to highlight the HIPAA risks if using a non-secure platform to communicate under extraordinary circumstances during the COVID-19 Pandemic.
- Discussion of costs related to the visit including permission to bill their insurance for this visit and further telemedicine visits that may be offered in the future.
- A statement that the consent was obtained by telephone including the reason, with the date and time including the names and relationships of any witnesses.
- If a form is used, explain how the consent was reviewed during the visit; and how they may obtain a copy, if one is not available at the time of the encounter.
- Confirmation that you gave the patient time to ask questions, documented how you answered them; what the patient said to verbalize their understanding of the consent; and that they wish to proceed.

RISK MANAGEMENT SAMPLE RESOURCES:

COVID-19 TELEHEALTH CONSENT FORM

DOWNLOAD WORD DOC TEMPLATE

DOWNLOAD FILLABLE PDF

INFORMED CONSENT FOR TELEMEDICINE SERVICES DURING COVID-19 PANDEMIC

Patient Name: _____	Date of Birth: _____	Medical Record #: _____
Physician Name: _____ Location: _____		Date Consent Discussed: _____

Telemedicine is the use of electronic information and communication technologies by a healthcare provider to deliver services to an individual when he/she is located at a different location than the healthcare provider. This may be for the purpose of diagnosis, treatment, follow-up and/or education. During your telemedicine consultation, details of your medical history and personal health information may be discussed with you or other health professionals through the use of interactive video, audio or other telecommunications technology. Additionally, a physical examination of you may take place, and video, audio, and/or photo recordings may be taken.

All efforts will be made to utilize electronic systems with network and software security protocols to protect the privacy and security of health information and to safeguard the data against corruption. However, in order to ensure greater access to care while limiting the spread of COVID-19, the mode of communication used during your telehealth consultation may not be secure and may be subject to privacy risks.

Anticipated Benefits:

- Improved access to medical care by enabling a patient to remain in his/her location while the healthcare provider provides care from a distant site
- Limiting the spread of COVID-19
- More efficient medical evaluation and management
- Ability to obtain consultation of a distant specialist
- Conservation of personal protective equipment such as gloves and masks to reduce shortages for healthcare providers

Possible Risks:

As with any medical procedure, there are potential risks associated with the use of telemedicine. These risks include, but may not be limited to:

- In rare cases, it may be determined that the information transmitted is of poor quality, requiring a face to face visit or rescheduled telemedicine visit. This may cause a delay in medical evaluation/treatment.
- Security protocols could fail or not be available, causing a breach of privacy of personal medical information.
- In rare cases, a lack of access to all of your medical records may result in adverse drug interactions or allergic reactions or other judgment errors.

Please initial after reading this page: _____

By Signing this Form, I Understand the Following:

1. I understand that I may expect the anticipated benefits from the use of telemedicine in my care, but that no results can be guaranteed.
2. I understand that all efforts will be taken to protect the privacy and security of health information, and that no information obtained in the use of telemedicine which identifies me will be intentionally disclosed to researchers or other entities without my authorization.
3. I understand that during the COVID-19 Pandemic, security measures may be lessened in accordance with U.S. Department of Health and Human Services (HHS) to ensure improved access to care.
4. I understand that I have the right to withhold or withdraw my consent to the use of telemedicine in the course of my care at any time without affecting my right to future care or treatment.
5. I understand there may be technological challenges that prevent recording the telemedicine interaction during the COVID-19 pandemic, but that I have the right to inspect all information obtained and successfully recorded and may receive copies of this information for a reasonable fee.
6. I understand that a variety of alternative methods of medical care may be available to me, and that I may choose one or more of these at any time. My healthcare provider has explained the alternative to my satisfaction.
7. I understand that the telemedicine visit may occur with a licensed medical provider who is not licensed in my state of residence. I also understand there may be electronic communication of my personal medical information to other medical providers who may be located in other states.
8. I understand that my healthcare information may be shared with other individuals for scheduling and billing purposes. Others may also be present during the consultation other than my healthcare provider and consulting healthcare provider in order to operate the video equipment. The above-mentioned people will all maintain confidentiality of the information obtained. I further understand that I will be informed of their presence in the consultation and thus will have the right to request the following: (1) omit specific details of my medical history/physical examination that are personally sensitive to me; (2) ask non-medical personnel to leave the telemedicine examination room; and/or (3) terminate the consultation at any time.
9. I understand that certain fees for service may be waived during the COVID-19 Pandemic depending on my insurance carrier. While all efforts will be made to follow guidelines during this fluid situation, I may be responsible for any copayments or coinsurances that apply, and if my medical insurance coverage is not sufficient to satisfy any excess cost, I will be responsible for payment.

Patient Consent to the Use of Telemedicine

I have read and understand the information provided above regarding telemedicine during the COVID-19 Pandemic. I have discussed and had an opportunity to ask my healthcare provider questions. All of these questions have been answered to my satisfaction.

I hereby **authorize** _____ (*name of physician*) to use telemedicine in the course of my diagnosis and treatment.

*Signature of Patient (or person authorized to sign for patient):*_____ *Date:* _____

If authorized signer,
Relationship to patient: _____

Witness: _____ *Date:* _____

I hereby **refuse** _____ (*name of physician*) to use telemedicine in the course of my diagnosis and treatment.

*Signature of Patient (or person authorized to sign for patient):*_____ *Date:* _____

If authorized signer,
Relationship to patient: _____

Witness: _____ *Date:* _____

I have been offered a copy of this consent form (patient's initials) _____

NORCAL GROUP®

BEST PRACTICES: RISK MANAGEMENT RESOURCE

TELEPHONE LIABILITY

Telephone communication offers patients greater accessibility to physicians and has become an integral part of office practices. It helps provide patients with needed clinical services in a way that uses resources efficiently. Patients are given the opportunity to get answers to questions; obtain test results, referrals and prescription refill authorizations; and receive necessary care in a timely manner.

Medical Professional Liability Risks

While the use of the telephone extends the physician's medical practice capabilities, it also expands risks. A telephone conversation cannot replace the results obtained from a physical examination of a patient. Malpractice suits have resulted from situations in which a patient's complaints of symptoms were handled by multiple phone conversations but no actual physician visits. Often in these cases, the patient reports vague, generalized symptoms, which may or may not represent a serious medical condition but which turn out to be indicative of an acute illness or problem — for example, meningitis in a pediatric patient, ectopic pregnancy in a woman of childbearing age, or myocardial infarction in a previously healthy but stressed 45-year-old man. If the physician elects not to immediately see a patient as a result of a telephone call, repeat calls and continued complaints should prompt a physical examination.

Inappropriate use of both licensed and unlicensed staff to respond to patient calls can result in patient harm and liability claims based on allegations of failure to supervise, improper delegation, and aiding and abetting the unlicensed practice of a profession. If not conducted properly, telephone screening is associated with many pitfalls (e.g., delayed communication, incomplete information, and screening and diagnostic errors) that could lead to patient harm and subsequent lawsuits. The following factors can make a practice's telephone screening process vulnerable to such pitfalls:

- Insufficient written screening protocols and/or training of unlicensed staff who answer patient calls.
- Poor communication skills on the part of the patient or staff and/or between staff and physicians.
- Insufficient or lack of standardized workflows for communication hand-off processes.
- Clinician unwillingness to supervise, review, assist and/or respond when patient calls require clinician involvement.
- Inadequate documentation of patient communication.

Telephone Triage vs. Telephone Screening

Telephone triage is the clinical management and determination of urgency of patients' health concerns and symptoms reported via a telephone interaction by a licensed health care professional whose scope of practice includes the performance of such assessments, for example a registered nurse. In physician practices that do not employ licensed health care professionals, initial patient contact often occurs with

unlicensed receptionists and medical assistants who answer calls, relay messages and schedule appointments. Caution needs to be exercised, therefore, when allowing unlicensed staff to conduct telephone screening of medical problems. Although some staff may have experience, it is outside the scope of unlicensed staff to triage clinical calls, and they should never be tasked to independently make assessments, decisions, or judgments regarding a patient's clinical care needs.

Imposing proper limitations on the scope of services of unlicensed staff creates a significant challenge for physician practices that do not employ registered or licensed professionals. This challenge can be addressed when physicians work collaboratively with their clinical staff and office administrator to develop policies and procedures for a telephone communication and screening system. This system would take into account the education, training and supervision requirements that are necessary to perform this function safely. The telephone screening system must work effectively to ensure that patients with clinical needs are directed to those whose scope of practice allows them to appropriately triage, advise, and/or determine further care needs

It is best that each practice have screening protocols for handling all types of patient calls: requests for appointments, prescription refills, patients asking to speak to their doctors, emergencies, critical test results, calls from other physicians, personal calls, billing problems, etc. Screening protocols will help staff to handle problems and inquiries efficiently and consistently.

It is especially important for office personnel to know when a call is an emergency situation. The staff should be able to recognize when a patient should be referred to the hospital emergency department, have immediate access to speak to a licensed professional, be seen by a physician sooner than the schedule will currently permit, and also what instructions to give to a patient, especially if the physicians in the practice are not in the office. If office personnel ever have any doubt about what to tell a patient on the phone, they should get as much information from the patient as possible and then consult with the immediate supervisor or a physician. Unlicensed office staff members must also be careful not to attempt to interpret or diagnose a patient's clinical condition or to independently provide medical advice over the phone in response to a patient's symptoms or concerns.

Documentation of Telephone Calls

Adequate written documentation of telephone calls is essential. Documentation of all telephone encounters should be treated with the same level of importance as documentation of in-person visits. Telephone conversations—especially those that occur after-hours—in which medical advice is communicated to the patient should always be documented. Without documentation of medically related telephone calls, continuity of care may be adversely affected.

A physician who cares for the patient after the patient has been treated over the phone is at a disadvantage if there is no record of the telephone treatment. Liability may arise if the absence of information in the medical record results in patient injury or a delay in diagnosis.

Revised: August 2018

It is also difficult to dispute allegations about a telephone conversation without a documented record. Lawsuits often occur years after care was rendered. Because of the length of time that has passed since that particular call, the physician will most likely not remember the facts of the call. If there is no documentation regarding the content of the call, the patient**,** or a loved one**,** can say anything about the content of the discussion without a verifiable dispute. This may make a case more difficult to defend.

Risk Management Recommendations

- Schedule staff hours so that you have adequate phone coverage at high-volume call times. Periodically have your office manager check to see that there are enough lines into the practice to ensure that patients do not get a busy signal for an extended period for time.
- Develop comprehensive job descriptions and protocols for staff, including explicit instructions regarding how calls should be handled and documented, and under what circumstances clinicians must be consulted. (See sample *Policy and Procedure Telephone Screening Documentation.)*
- Assess the staff member's competency to screen calls. Delegating this responsibility implies that the staff member has the appropriate training, competence and experience. This person must also have the authority and confidence to interrupt clinicians for assistance whenever needed.
- Detailed written guidelines should be available to guide the telephone screening process. Develop screening procedures addressing how to direct calls and how to respond to patient's clinical symptoms reported by phone. For example, the procedures should delineate how to respond when patients indicate they need immediate help, those that can be addressed by a non-clinician, and those that can wait for a return call (see sample *Telephone Decision Grid*).
    - Any calls in which the caller was advised to promptly dial 911 should immediately be reported to the physician.
- Train staff to urge patients to call back if their symptoms get worse or do not improve or if they have additional questions or concerns.
- Provide for prompt physician review of all telephone patient encounters including any calls not handled by a physician. Physician review shows that the doctor has evaluated for appropriateness of triage and documentation, made all medical decisions and that adequate supervision of unlicensed staff occurred. Careful review is especially important for those signs and symptoms that have been previously determined by the physician as being high risk.

Documentation of Telephone Contacts

- Document all patient-related phone calls and in-person encounters that occur both during and after office hours. This includes calls and encounters related to your own patients and those for whom you provide after-hours care when covering for another physician. Documentation should be clear and legible.
- Communications related to patient care should be documented, especially all calls in which patients report clinical symptoms Include the following information when utilizing any medical record format including an electronic health record's system for telephone encounters:

  - Patient's name
  - Caller's name
  - Return phone number
  - Name of the patient's primary physician
  - Date and time of call
  - Chief complaint and symptoms
  - Allergies/Reactions
  - Current medications
  - Disposition of call
  - Signature of person receiving the call (e.g., receptionist, medical assistant)
- When advice is provided over the telephone, document the following on the patient's telephone contact form:
  - Advice given to the patient
  - Date and time the call was returned and to whom
  - Signature and name of the licensed professional directing that advice, (e.g., physician, nurse practitioner, physician assistant)
- Demonstrate adequate supervision and physician involvement in telephone screening of problems by physician documentation on the form or review of electronic telephone encounters. Forms should include:
  - Date and time of review
  - Physician initials or signature
- Consider using a "Telephone Contact Form" (see sample) to help ensure complete documentation that accurately reflects all the clinical issues that were discussed in the telephone conversation. If a form is used, attach/scan it into the permanent record as soon as possible.
- Document patient-related phone calls with other healthcare providers (such as on-call physicians or managed care organizations) directly into the medical record, as soon as possible.
- When documenting telephone calls among healthcare professionals (emergency physicians, on-call physicians, and primary physicians), include the reason for the call, patient-related information communicated, requests for on-site evaluation, and requests for management or follow-up plans.
- When on-call, if you are a specialist, communicate the patient information to the primary attending physician and to the physician for whom you are on-call. Use fax, email, phone or electronic health records (EHR) systems as appropriate. Include the date and time of the communication.
- Document if patients are told to call back if there is no improvement in their condition or if they have additional symptoms. Include other details of telephone calls concerning prescription refills, reports of test results, and/or missed or canceled appointments.
- Document any follow-up calls made to check on the status of the patient, request to come into the office to be seen, and any referral to an urgent care center or a hospital emergency

department including the risks and possible consequences of failure to follow such advice as discussed with the patient.
- Document in a fashion that supports the decision-making process.

Additional Resources

- NORCAL risk management resources:
  - Telephone Liability: After-Hours Telephone Calls, Answering Services, and On Call Coverage
  - Allied Health Personnel: Unlicensed Assistive Personnel – Medical Assistants
  - Medical Assistant: Scope-at-a-Glance
    - Medical Assistant: Scope-at-a-Glance for California-based practices
  - Medical Assistant: Can and Cannot Do List
    - Medical Assistant: Can and Cannot Do List for California-based practices

Sample Form

- Telephone Decision Grid
- Telephone Contact Form
- After Hours/On Call Telephone Contact Form

Sample Policy and Procedure

- Telephone Screening and Documentation

Revised: August 2018

RISK MANAGEMENT SAMPLE RESOURCES:
GRIDS, DOCUMENTATION AND FORMS

- Sample Form: Telephone Decision Grid | ***Download Word Template***
- Sample Form: Telephone Contact Form | ***Download Word Template***
- Sample Form: After Hours/On Call Telephone Contact Form | ***Download Word Template***
- Sample Policy/Procedure: Telephone Screening and Documentation | ***Download Word Template***

Telephone Decision Grid

Instructions: After the physician marks the appropriate boxes, consider laminating this grid to keep by the phones. Ensure that all care-related conversations with patients are documented in the medical record. Below is a sample Telephone Decision Grid with examples of some types of calls. It is not all-inclusive. Questions should be developed by the physicians for the employee to ask as related to the symptoms.

Type of Calls	Obtain immediate physician response	Refer to hospital ED/ Advise pt. to call 911	Inform patient physician will call back ASAP	Obtain immediate APP response	Take message for RN or APP to return call same day	Make same-day appointment	Take message, physician will return call when available
I. Patient Symptoms							
Patient/Caller stated emergency							
Fever over: _____							
Chest pain							
Heavy bleeding							
Severe pain							
Shortness of breath							
Reaction to medication (describe reaction)							
Disoriented, confused							
Numbness in arm or leg							
Inability to urinate							
Vomiting							
Diarrhea							
Sore throat							
Contractions (pregnant)							

Revised: August 2018

Type of Calls	Obtain immediate physician response	Refer to hospital ED/ Advise pt. to call 911	Inform patient physician will call back ASAP	Obtain immediate APP response	Take message for RN or APP to return call same day	Make same-day appointment	Take message, physician will return call when available
II. Patient Requests							
Information on medical condition							
Test results							
Medication change/Question							
Copy of medical records							
Explanation of bill							
Health/Life/Disability insurance form (FMLA) completion							
Angry patient							
III. Other							
Admission to ED/Hospital							
Hospital staff with lab or test results							
Hospital with notification of change in patient condition							
Laboratory with test results							
Consulting physicians							
Insurance company or attorney requests							
NOTE: Add additional items to the lists above as needed and appropriate.							

Revised: August 2018

This sample is a template only and is not intended to be used "as is." It is an example to assist the policyholder in the development of a document that is tailored to the individual practice. This sample is intended solely for the use of NORCAL policyholders as reference material only. It does not constitute legal advice, but is intended to supplement risk management advice. You may want to have this information reviewed by an attorney to determine if it is appropriate for use in your practice or institution.

Telephone Contact Form

Patient's Name:		DOB:
Caller's Name/Relationship to Patient (if caller is NOT the patient):		Return Phone Number:
Date of Call:	Time of Call:	am/pm
Patient's Primary Physician:	Message Taken by:	
Reason for Call (chief complaint and symptoms if applicable):		
Allergies/Reactions:		❑ NKA
Current Medications:		

Disposition of Call:

❑ Referred to physician _____

❑ Referred to: _____

❑ Patient instructed to go to the ED ❑ Scheduled Appointment for Date: _____ Time: _____

❑ Other:

Clinician response/Advice/Information to be provided to patient:

FOLLOW UP SECTION

Message given to: ❑ Patient ❑ Caller (named above)

❑ Patient's representative/Other (Name): _____

Message/Advice relayed by:

Date: Time:

Physician Signature:

Date: Time:

Revised: August 2018

This sample is a template only and is not intended to be used "as is." It is an example to assist the policyholder in the development of a document that is tailored to the individual practice. This sample is intended solely for the use of NORCAL policyholders as reference material only. It does not constitute legal advice, but is intended to supplement risk management advice. You may want to have this information reviewed by an attorney to determine if it is appropriate for use in your practice or institution.

After Hours / On Call Telephone Contact Form

Patient Name: _____ Date/ Time of Call: _____

Caller Name (if other than patient: _____ Return Phone #:_____

Primary Physician: _____

Chief Complaint/Duration:_____

_____

Related Symptoms: _____

Recent tests/ procedures/ surgery: _____

Previous calls to other healthcare professionals about this or related complaints:

_____

_____

Allergies: _____

Current medications: _____

Other significant medical history: _____

Advice/instructions given/ treatment ordered/ prescriptions given: _____

_____

Patient expressed understanding of advice/ instructions: Yes _____ No _____

Pharmacy: _____ Phone #: _____

Follow-up plan: _____

Information provided to primary physician (physician who is being covered): Yes _____ No _____

Date/ time information communicated: _____

Covering Physician Name (please print): _____

Signature: _____

Revised: August 2018

This sample is a template only and is not intended to be used "as is." It is an example to assist the policyholder in the development of a document that is tailored to the individual practice. This sample is intended solely for the use of NORCAL policyholders as reference material only. It does not constitute legal advice, but is intended to supplement risk management advice. You may want to have this information reviewed by an attorney to determine if it is appropriate for use in your practice or institution.

Subject: Telephone Screening and Documentation

Effective Date: **Revised Date:**

Approved by:

Policy

Staff members who screen telephone calls are to refer to the telephone decision grid when patients report specific signs and symptoms to determine who should address the patient's concern. Staff members are to document all patient care-related telephone contacts. Clinicians provide telephone advice and review **all** telephone encounters.

Purpose

Ensure that staff members, including medical assistants and receptionists, **screen** patient calls under the direction of the physician without making independent medical decisions. Ensure that all care-related conversations with patients are documented in the medical record.

Definitions

Telephone screening is the process of directing calls when patients report specific signs and symptoms by phone. Telephone screeners follow a checklist developed by a physician. The checklist outlines those signs or symptoms that require immediate response by a clinician, those that can be addressed by a non-clinician and those that can wait for a return call or scheduled visit (*see Telephone Decision Grid*).

Telephone triage is determining the clinical urgency of patient health concerns and symptoms reported via a telephone interaction completed by a licensed health care professional authorized to make an assessment. Telephone triage professionals utilize protocols or guidelines, in paper or electronic format, to help sort symptoms, from "chest pain to chicken pox," ranking patient's health problems according to their urgency and making safe, effective, and appropriate dispositions of telephone interactions.

Telephone screening is not to be confused with telephone triage.

Procedure:

Staff members:

- Document all patient healthcare-related telephone calls particularly when patients report a sign or symptom (see sample *Telephone Contact Documentation Form* or input per electronic health record system) Include the following information:
    - Patient's name
    - Caller's name
    - Return phone number
    - Name of the patient's primary physician
    - Date and time of call
    - Chief complaint and symptoms
    - Allergies/Reactions
    - Current medications
    - Disposition of call
    - Signature
- Refer to the telephone decision grid to determine who should address the patient's concern. Whenever the patient's concern is unclear or not addressed on the telephone decision grid, a clinician should determine who should handle the patient's call.
- When referring a call to a clinician, ensure the patient medical record as well as the telephone contact form documentation is available for their access and review during the call.

Physicians:

- When providing advice over the telephone, document the following on the patient's telephone contact/electronic phone encounter form:
    - Advice given to the patient
    - Date and time the call was returned and to whom
    - Signature
- Review **all** telephone patient encounters. Physician review shows that the doctor made all medical decisions and that adequate supervision of staff members occurred. Careful review is especially important for those encounters that have been previously determined by the physician as being high risk.
- Document the date and time, and either initial or sign the telephone contact form to demonstrate adequate supervision and physician involvement in telephone screening of problems.

Revised: August 2018

BEST PRACTICES: RISK MANAGEMENT RESOURCE

TELEPHONE LIABILITY: AFTER HOURS TELEPHONE CALLS, ANSWERING SERVICES AND ON CALL COVERAGE

After-hours care can present challenges to ongoing successful patient treatment and continuity of patient care. On-call providers may have little or no advance information concerning the patient's condition when responding to a patient's phone call. Patients are frequently unaware of whether their condition is a life-threatening emergency and can be reluctant to call 911. Finally, patients often access on-call providers through voicemail or answering services, which are commonly staffed with non-medical personnel who do not have the expertise or license to assess a patient's condition.

Although it is not generally mandated that a physician provide back-up or on-call coverage when unavailable, to avoid a potential allegation of abandonment, it is prudent to provide patients with appropriate medical backup care during an absence. Continuity of care is a professional responsibility for physicians. Assisting patients with access to care outside of normal business hours when the severity and acuteness of a patient's medical condition warrants intervention is part of that responsibility. Depending on the physician's specialty and the nature of the patient's problem, it may not be considered adequate for the physician simply to direct patients to the nearest emergency department after hours. According to a study cited in the *Journal of Family Practice*, some patients have difficulty determining if their problem warrants immediate physician attention or fail to "persevere long enough to overcome system barriers that prevent them from talking to a physician," such as dealing with an answering machine or making a second phone call. (Hildebrandt D. After-hours telephone triage effects patient safety. *J Fam Pract.* 2003 March;52(3):222-228. Available at: www.mdedge.com/jfponline/article/60127/after-hours-telephone-triage-affects-patient-safety (accessed 6/22/18)).

Failure to make specific arrangements for after-hours coverage may lead to allegations of abandonment of patients and/or delays in diagnosis and treatment. Conversely, when answering services work well and patients understand how to use them, continuity of care is enhanced and physician liability is reduced. Accordingly, all physicians are strongly encouraged to participate in an after-hours call or coverage arrangement allowing for the provision of urgent care to their patients.

Medical Professional Liability Risks

Patient harm can occur—possibly leading to allegations of malpractice—when answering services are confusing or do not facilitate timely contact with a physician. It can also occur when a patient does talk to an on-call provider and the provider, without access to the patient's medical record, tries to rely on memory of the patient and record, as well as when there is failure to properly document the after-hours contact in the patient's medical record.

Some health plans have requirements that participating physicians provide after-hours coverage for patients. Practices designated as medical homes may also be required to provide access to care "24/7" in order to meet the program requirements. In addition, the state in which you practice may have regulations or have adopted standards relating to the provision of after-hours care. For example, Alaska has adopted the "reasonable patient standard" doctrine with respect to physician-patient communication and informed consent based on the precedent-setting case *Marsingill v. O'Malley*. The

Marsingill case established that it is the duty of a physician receiving an after-hours patient phone call to provide sufficient information to the patient to make an informed decision regarding necessary follow up, including the possible consequences to the patient that could arise if the patient fails to follow the physician's advice. [128 P.3d 151, *Marsingill v. O'Malley*, (Alaska 2006)]

Providing On-Call Coverage

There are other on-call coverage systems available that may increase access to after-hours care besides the traditional "physicians taking turns". Improved patient outcomes and lowered use of the emergency department is associated with receiving care outside of routine business hours. Assessing your patient demand and provider capacity will assist you in creating a system to improve access to care. Also take into consideration the availability of a shared health record and other methods of notification for maintaining continuity of care. (O'Malley, A. After-Hours Care and its Coordination with Primary Care in the U.S. *J Gen Intern Med.* 2012 Nov; 27(11): 1406-1415. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3475839/ (accessed 06/25/18)

Although this is not all-inclusive, some examples of coordinated access to after-hours care are listed below and may be an appropriate method of providing coverage depending on your specialty and the circumstances:

- Contract with nurse triage answering services or call centers
- Make arrangements with urgent care clinics, walk-in clinics, after hours student health centers or other services with expanded hours
- Work together with local physicians to provide a service; with multiple physicians involved the cost can be shared
- Hire a part time physician or advanced practice professional to provide extended office hours, including some evenings and weekends.
- Utilize locum tenens to extend office hours
- Hire a professional after-hours call center that offers phone call coverage with immediate access to a Board Certified physician or Advanced Practice Professional.
- Consider contracting with a telemedicine or video telehealth company for extended coverage

An optimal coverage arrangement includes providing instructions to patients for accessing after-hours coverage offered by a qualified, trained healthcare professional able to assess and direct the patient based on need, in addition to providing follow up information to the PCP.

Risk Management Recommendations

The following risk management recommendations apply for any type of after-hours coverage.

- Document and maintain all patient interactions, including telephone encounters, even when on call or after-hours.
    - Ensure that on-call physicians and midlevel practitioners who provide after-hours coverage thoroughly document phone calls.

  - Document and maintain answering service and answering machine/voicemail messages the same way that you document office calls, placing a copy of the documentation in the patient's chart the next day.
- Ensure that appropriate, standardized coordination of care and communication occurs.
  - Provide information to on-call partners and primary treating physicians regarding the management of patients in a timely fashion by fax, email, phone or entry into electronic health system (EHR).
- Consider using one of the following systems to ensure prompt documentation of after-hours calls:
  - If dictation is used, dictate directly to your dictation system. Once transcribed, review notes for accuracy, sign, date, and appropriately file into the medical record if no further action is needed for the patient.
  - If a smart phone is used for notes or recordings, have a process in place for transferring the information to the medical record and then deleting it from the smart phone. Only use HITECH compliant smartphone devices.
  - Keep an index card or telephone message pad in your pocket. Note the substance of the call at the time it occurs, and document in the patient's medical record when you get to the office, including the time and date.
  - If access is available to an EHR, document directly into the system at the time that the call is taken.
- Provide patient education about after-hours calls by distributing information in a brief handout or include such information in practice brochures and new patient packets.
  - Practice business hours
  - After-hours phone number(s)
  - Who will be taking patient calls (e.g., an answering service that will page an on-call physician)
  - How a patient should use the answering service (e.g., state need or chief complaint clearly, speak slowly, state name of physician whom patient is calling, state telephone number where patient can be reached)
  - When a patient should call back if he or she has not received a return call from the physician (e.g., patient should call back if he or she has not received a return call from the physician within 30 minutes)
- When opting for physician on-call coverage use on-call physicians who practice the same specialty
- Establish a hand-off procedure when there is cross coverage with other physicians to ensure an exchange of information about patients who may require care.
- Because it is difficult to diagnose a medical condition over the telephone (i.e., the physician may have no access to the patient's medical records and cannot perform a physical examination), encourage on-call physicians to maintain a low threshold for directing patients to urgent care centers or hospital emergency departments, depending on the nature of the complaint.

- Document requests for the patient to come into the office to be seen and any referrals to urgent care centers or hospital emergency departments and the possible consequences discussed with the patient of failure to follow such advice.
- Provide the patient sufficient information to make an informed decision regarding necessary follow up, including the possible consequences to the patient that could arise if the patient fails to follow the physician's advice.

Answering services

- Develop a policy and procedure pertaining to after-hours calls and the answering service.
    - Have a log or report of answering service calls faxed to the office each morning.
    - Ensure that these calls were handled appropriately and that patients' needs were addressed.
    - Use on-call notes to document the call and information discussed.
    - Assign a staff member to check the list and verify that each patient issue has been addressed (e.g. patient called, scheduled to be seen or has received advice or intervention) and the communication has been documented.
    - Periodically review these calls with the answering service.
- Ensure that all answering service logs are retained as long as medical records are retained according to state guidelines.
- Instruct answering services to identify themselves as such.
- Notify the answering service of the physician(s) who will be on-call for specific days of the week. Update the answering service about any changes when you leave the office.
- Instruct the answering service on how and when to contact the on-call physician(s) and what to do if there is no response (e.g., locate a designated alternate physician when the on-call physician cannot be reached).
- Provide the answering service with contact information for on-call and back-up physicians or advanced practice providers (e.g., pager numbers and cell phone numbers).
- As appropriate, instruct the answering service to send clinical calls to a designated trained individual for triage, if not directly to the physician.
- Instruct the answering service how to direct patients to emergency care (e.g., dial 911 or go to the nearest emergency department).
- Ensure that the answering service complies with the Health Insurance Portability and Accountability Act (HIPAA) and state privacy regulations.
- Contact organizations such as local medical societies or the Medical Group Management Association (MGMA) for answering service resources, as there are a variety of services that employ different levels of technology.

Answering machines

- Ensure you understand the risks associated with the lack of after-hours on-call coverage and the use of only an answering machine for after-hours calls.

- Design the after-hours voicemail systems so ideally patients are not required to call a second number, or choose from too many options, or to make a judgment as to whether or not they need to speak to a physician. If the patient has to call a second number, ensure that someone is available to take the call.
- Rather than having the answering machine instruct patients to leave a message only or go to the emergency room, record instructions explaining how your patients can reach the on-call physician, triage nurse or answering service depending upon your coverage arrangement.
- Establish a reasonable timeframe for returning messages or pages (e.g., same day, within several hours, within 30 minutes).
- Ensure that the answering machine or voicemail system has good storage capacity and message retrieval capability.
- When on-call, check for after-hours messages at regular intervals.
- Consider using a "Telephone Contact Form" (see sample) to help ensure complete documentation that accurately reflects all the clinical issues that were discussed in the telephone conversation. If a form is used, attach it to the permanent record as soon as possible. When using an EHR set up the system to capture these elements.

Additional Resources

NORCAL's risk management resource Telephone Liability

Sample Form

After-Hours/On-Call Telephone Contact Form

Revised: August 2018

After Hours / On Call Telephone Contact Form

Patient Name: _____ Date/ Time of Call: _____

Caller Name (if other than patient: _____ Return Phone #:_____

Primary Physician: _____

Chief Complaint/Duration:_____

_____

Related Symptoms: _____

Recent tests/ procedures/ surgery: _____

Previous calls to other healthcare professionals about this or related complaints:

_____

_____

Allergies: _____

Current medications: _____

Other significant medical history: _____

Advice/instructions given/ treatment ordered/ prescriptions given: _____

_____

Patient expressed understanding of advice/ instructions: Yes _____ No _____

Pharmacy: _____ Phone #: _____

Follow-up plan: _____

Information provided to primary physician (physician who is being covered): Yes _____ No _____

Date/ time information communicated: _____

Covering Physician Name (please print): _____

Signature: _____

Revised: August 2018

This sample is a template only and is not intended to be used "as is." It is an example to assist the policyholder in the development of a document that is tailored to the individual practice. This sample is intended solely for the use of NORCAL policyholders as reference material only. It does not constitute legal advice, but is intended to supplement risk management advice. You may want to have this information reviewed by an attorney to determine if it is appropriate for use in your practice or institution.

NORCAL GROUP®

BEST PRACTICES: RISK MANAGEMENT RESOURCE

COMMUNICATION: TEXTING IN THE HEALTHCARE SETTING

Texting has become a major mode of communication in today's society. Not only are there clear advantages from a social standpoint, texting can also have value in the healthcare setting. In response to the demands of high patient caseloads and acuity in patients, clinicians are embracing technology that enhances communication, reduces paperwork, and synthesizes information in a manner that is manageable. To that end, texting is fast, direct, simplifies the traditional pager and call-back system, and can be used to facilitate quick communication with clinicians, staff, and even patients.

Unfortunately, traditional texting is not compliant with the security and privacy regulations under HIPAA and HITECH and also brings with it a host of quality, accuracy, documentation, and operational concerns that should be addressed by risk management. Most facilities are aware of the proliferation of texting and will often write policies to address it, but they have a limited ability to stop its use in the healthcare setting. So rather than prohibiting texting, it is important to consider addressing its use with the appropriate solutions and policies in place.

Risk Management Considerations / Medical Professional Liability Risks

Communication with Clinicians and Other Caregivers

Texting helps facilitate communication with other clinicians and staff. It is believed that texting can reduce wait times on callbacks and test results, and improve the efficiency of communication. However, it is important to remember that texting should never replace a phone call when important information needs to be exchanged. Phone conversations allow for important information to be exchanged with greater ease, more natural opportunity for questions and responses, and a reduction in the opportunities for mistakes that occur with electronic messaging, especially texting. Text messages should not be used for urgent situations or if there is the need to know instantaneously that the communication has been received.

As technology and security of mobile devices has evolved, The Joint Commission's (TJC) position on texting orders has also evolved. In May of 2016, TJC briefly lifted the ban on texting orders. However, in a Joint Commission announcement shortly after they rescinded the ban, TJC delayed the implementation of texting orders based on a determination that further guidance was needed. In December 2016, The Joint Commission updated its guidance after collaborating with the Centers for Medicare and Medicaid Services (CMS) reporting that its ban on using secure text messages to transmit patient care orders would stay in place. Finally, in a CMS Survey and Certification memo of December 28, 2017, the agency clarified that care team members are allowed to text patient information over a secure messaging app but texting medical orders is still banned, i.e., it is not in compliance with CMS Conditions of Participation (CoPs) or its Conditions for Coverage (CfCs). It noted that Computerized Provider Order Entry (CPOE) is the preferred method of order entry. According to CMS, systems/platforms must be secure, encrypted and minimize risks to patient privacy and confidentiality as per HIPAA regulations to be compliant with the CoPs or CfCs. A secure platform should include elements such as secure sign-on, message encryption, delivery and read receipts, date and time stamps,

criteria for message retention, and a specified contact list for individuals authorized to receive and record orders.

Communication with Patients

Some physicians, medical offices, and healthcare institutions are communicating directly with patients through text messages. These electronic messages could include text alerts for normal test values, check-in after an appointment, and reminders to get diagnostic testing or make appointments. Some offices are finding that shorter messages may assist in conveying quick information that does not require explanation, and that it aids in staff productivity. However, texting can become a nuisance and ignored if over-utilized.

Privacy and Security Issues

Given the rise in enforcement of compliance with HIPAA and HITECH, healthcare facilities should address texting as part of the HIPAA-required risk analysis and implement "reasonable and appropriate" security measures to control and minimize the risks.

Facilities and clinicians texting PHI without proper safety and encryption processes in place could result in HIPAA and HITECH violations and breaches of confidentiality. Tiered penalties can range from $100 to $50,000 per violation, up to a maximum of $1.5 million per year for violations of an identical provision, so violations can represent a real financial risk to facilities.

Devices

The protection of information is challenging when utilizing handheld devices such as cellphones, smartphones, or tablets for the purposes of electronic communication. With all of the available data, these devices risk unauthorized access, use, and/or disclosure of PHI due to theft or loss of the device, improper disposal, access by an unauthorized individual, and even signal interception. Although the highest risk is theft or loss of the device, the American Health Information Management Association (AHIMA) stated there is inexpensive equipment and software available to the public that easily allows for the interception, decryption, and forwarding of text messages.

"Distracted Doctoring" and the Accuracy of Texts

Texting errors are a significant concern when using electronic communication. Most of these errors are related to distractions, multi-tasking, unapproved text shorthand, and autocorrect on smart phones. Distractions and multi-tasking constitute a real concern, and multiple media outlets have reported on it. Some sobering examples from an article in *The New York Times*: half of surveyed technicians acknowledged texting during surgery while they were responsible for running bypass machines; texting occurred during emergencies; and one physician forgot to complete a cardiac medication order because she was distracted by a personal text, which resulted in unnecessary cardiac surgery for the patient. The issue has been coined "distracted doctoring" and is noted to be intensifying throughout the country even though facilities are enacting more and more stringent policies to address it.

The Institute for Safe Medication Practices (ISMP) reports inappropriate use of texting abbreviations not recognized by the healthcare industry. One example ISMP cites is an order sent to a hospital pharmacy

from a nurse that stated “Slomag, 64mg TID, 2Day.” The pharmacist called the nurse to clarify the order, and the nurse stated it was for SLOW-MAG (magnesium chloride) and “2Day” is text shorthand for “today.” It was confirmed that the nurse had directly transcribed the order to the medical record from a text she received. Other text shorthand examples include “B4” (before), “c” (see), “ez” (easy), “w8” (wait), “r” (are), “imo” (in my opinion), “u” (you), “a/s/p” (age, sex, problem), “b4n” (bye for now), and “l8r” (later). Obviously, the use of unapproved text shorthand and abbreviations as well as typos or inappropriately auto corrected text can easily result in errors in patient care and increase the opportunities for miscommunication.

Documentation

A significant concern related to text messages is how information used for medical decision-making can be efficiently and effectively incorporated into the medical record. All communications with or about patients’ healthcare and treatment, whether in face-to-face conversation, by phone, fax, email or text, should be documented in the medical record.

Retention of Texts

Texts are saved by the telecommunications carriers and can be requested and printed. This is referred to as metadata (the data behind the data). Just because a user erases something on his or her phone does not mean it is gone. Consequently, malpractice attorneys can subpoena the text messages of all involved clinicians in a malpractice claim from the telecommunications providers.

Texts can also be maintained on a phone indefinitely. Some individuals save text messages to have proof of their action or if they are concerned about potential outcomes and want to have something to defend their action should allegations arise.

Risk Management Recommendations

The following recommendations may help clinicians address the risks associated with texting:

- Designate an individual who is knowledgeable and experienced in privacy issues as the privacy officer to monitor compliance with this and other privacy issues.
- Develop a policy and procedure that either prohibits the texting of PHI or limits what information can be texted and implements precautions to ensure appropriate HIPAA, HITECH, and documentation compliance.
- Ensure appropriate HIPAA, HITECH, and documentation compliance protocols are understood and followed.
- Educate healthcare staff on risks (including the potential for personal and business-related monetary fines) associated with HIPAA and HITECH violations.
- Develop a comprehensive risk analysis and management strategy that identifies areas of vulnerability, implementation of “reasonable and appropriate” security measures, and monitoring systems in place to mitigate risk.

- Consider alternative secure electronic messaging technologies. Evaluate programs that allow for texting through secure portals, support HIPAA compliance, and allow for the logging and retrieval of texts for inclusion in the medical record. There are different examples on the market with varying levels of success.
- Address electronic messaging in medical staff by-laws.

Privacy Compliance

If the facility allows for the electronic messaging of PHI, the following issues should be addressed in a privacy policy or comprehensive risk analysis and management strategy:

- Electronic messages with PHI should only be sent by devices that are compliant with HIPAA and HITECH standards and encryption requirements. All devices that create, receive or store electronic communication containing PHI should require password protection and encryption.
- Any electronic message sent should be limited to the minimum information necessary for the permitted purpose. Any device that is discontinued or recycled should have all the information wiped, either at the source or remotely. No PHI data should be left on the device.
- Be sure to know whom you are texting since inadvertent texts can be a HIPAA violation.
- Do not send highly sensitive PHI (e.g., mental health, HIV, substance abuse, minor) through electronic messaging.
- Use smart phones or applications that are set up or provided by the facility. If using a personal smartphone, ensure that the facility's IT department has approved it and that it meets all the privacy standards.
- Notify the privacy officer if a device is lost, stolen, or replaced.
- Ensure that misdirected text messages are documented in the HIPAA disclosure log.
- Phones not used for a designated time-period, usually 1-3 minutes, should automatically lock and require a password to access the device.
- Phones that are stolen, lost, or are being retired should have the ability to be remotely erased of all e-mails and texts that contain PHI.
- Ensure that you have cyber-liability insurance coverage for potential exposures.

Accuracy of information

- Confirm the recipient of your text.
- Confirm delivery and receipt of the text. A confirmation receipt that the information was received is a good idea.
- Do not use shorthand or abbreviations.
- Use patient's full name and second unique identifier.
- Review texts prior to sending to ensure accuracy. Beware of autocorrect functions.
- Abide by CMS/Joint Commission policies regarding texting orders.

Documentation

- Develop a system to ensure that all text messages that are used for clinical decision-making are documented in the medical record.
- Utilize programs that integrate patient-related texted communications into a record-keeping system.

Additional Resources/References

- Greene, A.H. (2012). HIPAA Compliance for Clinical Texting. *AHIMA*. Available at: library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049460.hcsp?dDocName=bok1_049460 (accessed 4/4/19).
- U.S. Health and Human Services Office of Civil Rights Breach Portal. *Breaches Affecting 500 or More Individuals.* Report available at: ocrportal.hhs.gov/ocr/breach/breach_report.jsf (accessed 4/4/19).
- Centers for Medicare and Medicaid Services (CMS) memorandum regarding Texting of Patient Information among Healthcare Providers, December 28, 2017. Available at: https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-18-10.pdf (accessed 4/4/19).
- Richtel, M. (2011, Dec. 14). As doctors use more devices, potential for distraction grows. *The New York Times*. Available at: www.nytimes.com/2011/12/15/health/as-doctors-use-more-devices-potential-for-distraction-grows.html?_r=3&pagewanted=print (accessed 4/4/19).
- Tomes, J.P. (2015, Aug. 13). More on Texting! HIPAA & HITECH Act Blog. *Veteran's Press, Inc.* Available at: https://www.veteranspress.com/more-on-texting (accessed 4/4/19).

ABOUT NORCAL GROUP

The NORCAL Group of companies provide medical professional liability insurance, risk management solutions and provider wellness resources to physicians, healthcare extenders, medical groups, hospitals, community clinics, and allied healthcare facilities throughout the country. NORCAL Group includes NORCAL Mutual Insurance Company and its affiliated insurance companies. Please visit norcal-group.com/companies for more information.

Revised: June 2019

BEST PRACTICES: RISK MANAGEMENT RESOURCE

COMMUNICATION: EMAIL MANAGEMENT AND LIABILITY

Electronic communication, because it offers patients greater accessibility to physicians, has become an integral part of office practices. This tool helps provide patients with needed clinical services in a way that uses resources efficiently. Patients can get answers to questions and obtain test results, referrals and prescription refill authorizations in a timely manner.

While the use of electronic (email) communication extends the physician's medical practice capabilities, it also extends risks; therefore, documenting all email encounters should be treated with the same level of importance as documenting in-person visits.

Email should only be used to enhance the physician-patient relationship and not replace interpersonal contacts. There must be policies in place to ensure patients using email have consented to communicate electronically as well as to protect their confidentiality. The federal HIPAA Security Rule requires and enforces such protections.

All patient-care-related emails should become a part of the medical record. These might include emails between clinician and patient as well as emails between healthcare providers. Caution should be taken when healthcare providers utilize email as a means to communicate consultations, as these should always be formally structured.

If not adequately protected, emails may be read by unauthorized recipients (e.g., hackers, unintended email addressees, and imposters). Also, having test results delivered via email without adequate follow-up processes can actually increase the chance that a physician may not receive significant results. It is important to have a policy in place that describes how frequently practitioners must check their inboxes and the process by which results are then communicated to the various parties who need to see them.

Medical Professional Liability Risks

Although an easy and convenient communication process, email presents the practitioner with a number of risks in the clinical setting. These risks include:

- Security-related challenges (for example, emails that have poor/no encryption)
- Ambiguous or incomplete messages resulting in inadequate information for decision making
- Poor ability to track follow-up and to determine whether incoming and outgoing email messages were read
- Lack of methods to integrate emails into clinic workflow operations and/or medical records

(For further discussion of these and other risks, see the Katz and Moyer article cited under Additional Resources at the end of this document.)

In addition, exchanging emails with people who are not established as patients could expose the physician to allegations that a "physician-patient relationship" was created because of the response. Having a standard reply to emails from people who are not patients can indicate that the practice does not provide email consultations for anyone other than established patients. Importantly, even with a reply stating the email communication does not create a physician-patient relationship; such a

disclaimer may not be effective if the communication also provides medical advice. For example, a response to the sender suggesting that he/she make an office appointment could imply to the person that a physician-patient relationship is being initiated.

Risk Management Recommendations

The Appendix at the end of this article contains additional email communication recommendations from the American Medical Association.

General Email Communication

- Never use email for communications that require urgent or emergent hand-off information.
- As practicable, limit personal health information (PHI) contained in email correspondence.
- Encrypt all electronic transfers of confidential medical information and have security policies in place.
- Use firewalls and password protection to ensure that only designated users can gain access to emails.
- Maintain common courtesy and professionalism in all email correspondence.
- Double-check "to", "cc", "bcc", and "reply to all" fields before sending messages or replying to emails.
- Use automatic signature including name and contact information.
- Document all email correspondence. Place emails containing patient information or pertaining to patient treatment directly into the medical record.
- Ensure the medical record is updated to reflect changes or new information derived from an email communication (e.g. new or changed medication or allergy issues).
- Never assume an email has been read by the recipient. Any critical information (or information requiring an action on the part of the recipient) should NOT be communicated via email.
- Request a response verifying receipt of an email. If an action is required on the part of the recipient (schedule an appointment, call back, etc.), institute a follow-up process to make sure that action has been taken.
- Retain email failure messages (rather than deleting them) when transmissions are unsuccessful, and then use alternative means to contact the patient. Email fails for a variety of reasons (wrong addresses, system blocks, various technical issues, etc.). Retaining failure messages may help in the defense of a claim if there is some question as to why message transmission was unsuccessful.
- Establish a policy that details how frequently practitioners must check their inboxes and the process by which results are then communicated to the various parties who need to see them.
- Establish a policy specifying the parameters for email correspondence in your practice.
    - To see an example of a sample policy, go to: www.aafp.org/dam/AAFP/documents/practice_management/pcmh/healthit/EmailPolicyTemplate.doc (accessed 5/22/18).
- Backup email into long-term storage at least weekly.

Revised: August 2018

Email Communication between Physician and Patient

- Provide patients with guidelines for appropriate use of email communication (e.g., non-urgent messages, appointment scheduling, limitations on volume of email, response timeframes, etc.).
- Use patient portals whenever possible for email communication with patients.
- Obtain patients' written consent for email communication.
- Do not provide any advice or guidance that would normally be based on a physical exam and history.

Email Communication between Colleagues

- Use automatic reply function to let colleagues know you have received their email. When emailing colleagues, ask them to acknowledge receipt of your messages.
    - Automatic messages should communicate the timeframe in which your colleague should expect to receive a specific, personal response.
- Do not use email when immediate response is necessary.
- Clearly state action requests and response timeframes.
- Separate unrelated topics or patients into separate messages.

Additional Resources

- American Academy of Family Physicians. Sample email policy. www.aafp.org/dam/AAFP/documents/practice_management/pcmh/healthit/EmailPolicyTemplate.doc (accessed 5/22/18).
- American Medical Association. HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information. Available at: www.medicaltechnologyinsight.com/hipaa-phi-encryption.pdf (accessed 5/22/18).
- Katz SJ, Moyer CA. The emerging role of online communication between patients and their providers. Journal of General Internal Medicine. 2004;19(9):978-983. Available at: www.ncbi.nlm.nih.gov/pmc/articles/PMC1492520/ (accessed 5/22/18).
- Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. *Your Mobile Device and Health Information Privacy and Security*. Available at: www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security (accessed 5/22/18).

Revised: August 2018

Appendix

The following information is reproduced with permission from the American Medical Association web site (www.ama-assn.org). Copyright © 2018 American Medical Association. All rights reserved.

AMA Code of Medical Ethics Opinion 2.3.1 – Electronic Communication with Patients

Electronic communication, such as email or text messaging, can be a useful tool in the practice of medicine and can facilitate communication within a patient-physician relationship. However, these channels can raise special concerns about privacy and confidentiality, particularly when sensitive information is to be communicated. When physicians engage in electronic communication they hold the same ethical responsibilities to patients as they do during other clinical encounters. Any method of communication, virtual, telephonic, or in person, should be appropriate to the patient's clinical need and to the information being conveyed.

Email correspondence should not be used to establish a patient-physician relationship. Rather email should supplement other, more personal encounters.

Physicians who choose to communicate electronically with patients should:

a. Uphold professional standards of confidentiality and protection of privacy, security, and integrity of patient information.
b. Notify the patient of the inherent limitations of electronic communication, including possible breach of privacy or confidentiality, difficulty in validating the identity of the parties, and possible delays in response. Such disclaimers do not absolve physicians of responsibility to protect the patient's interests. Patients should have the opportunity to accept or decline electronic communication before privileged information is transmitted. The patient's decision to accept or decline email communication containing privileged information should be documented in the medical record.
c. Advise the patient of the limitations of these channels when a patient initiates electronic communication.
d. Obtain the patient's consent to continue electronic communication when a patient initiates electronic communication.
e. Present medical information in a manner that meets professional standards. Diagnostic or therapeutic services must conform to accepted clinical standards.
f. Be aware of relevant laws that determine when a patient-physician relationship has been established.

Revised: August 2018

AMA H-478.997 Guidelines for Patient-Physician Electronic Mail

New communication technologies must never replace the crucial interpersonal contacts that are the very basis of the patient-physician relationship. Rather, electronic mail and other forms of Internet communication should be used to enhance such contacts. Furthermore, before using electronic mail or other electronic communication tools, physicians should consider Health Information Portability and Accountability Act (HIPAA) requirements as well as related AMA policy on privacy and confidentiality, including Policies H-315.978 and H-315.989. Patient-physician electronic mail is defined as computer-based communication between physicians and patients within a professional relationship, in which the physician has taken on an explicit measure of responsibility for the patient's care. These guidelines do not address communication between physicians and consumers in which no ongoing professional relationship exists, as in an online discussion group or a public support forum.

(1) For those physicians who choose to utilize e-mail for selected patient and medical practice communications, the following guidelines be adopted.

Communication Guidelines:

(a) Establish turnaround time for messages. Exercise caution when using e-mail for urgent matters. (b) Inform patient about privacy issues. (c) Patients should know who besides addressee processes messages during addressee's usual business hours and during addressee's vacation or illness. (d) Whenever possible and appropriate, physicians should retain electronic and/or paper copies of e-mail communications with patients. (e) Establish types of transactions (prescription refill, appointment scheduling, etc.) and sensitivity of subject matter (HIV, mental health, etc.) permitted over e-mail. (f) Instruct patients to put the category of transaction in the subject line of the message for filtering: prescription, appointment, medical advice, billing question. (g) Request that patients put their name and patient identification number in the body of the message. (h) Configure automatic reply to acknowledge receipt of messages. (i) Send a new message to inform patient of completion of request. (j) Request that patients use autoreply feature to acknowledge reading clinicians message. (k) Develop archival and retrieval mechanisms. (l) Maintain a mailing list of patients, but do not send group mailings where recipients are visible to each other. Use blind copy feature in software. (m) Avoid anger, sarcasm, harsh criticism, and libelous references to third parties in messages. (n) Append a standard block of text to the end of e-mail messages to patients, which contains the physician's full name, contact information, and reminders about security and the importance of alternative forms of communication for emergencies. (o) Explain to patients that their messages should be concise. (p) When e-mail messages become too lengthy or the correspondence is prolonged, notify patients to come in to discuss or call them. (q) Remind patients when they do not adhere to the guidelines. (r) For patients who repeatedly do not adhere to the guidelines, it is acceptable to terminate the e-mail relationship.

Medicolegal and Administrative Guidelines:

(a) Develop a patient-clinician agreement for the informed consent for the use of e-mail. This should be discussed with and signed by the patient and documented in the medical record. Provide patients with a copy of the agreement. Agreement should contain the following: (b) Terms in communication guidelines (stated above). (c) Provide instructions for when and how to convert to phone calls and office visits. (d)

Describe security mechanisms in place. (e) Hold harmless the health care institution for information loss due to technical failures. (f) Waive encryption requirement, if any, at patient's insistence. (g) Describe security mechanisms in place including: (h) Using a password-protected screen saver for all desktop workstations in the office, hospital, and at home. (i) Never forwarding patient-identifiable information to a third party without the patient's express permission. (j) Never using patient's e-mail address in a marketing scheme. (k) Not sharing professional e-mail accounts with family members. (l) Not using unencrypted wireless communications with patient-identifiable information. (m) Double-checking all "To" fields prior to sending messages. (n) Perform at least weekly backups of e-mail onto long-term storage. Define long-term as the term applicable to paper records. (o) Commit policy decisions to writing and electronic form.

(2) The policies and procedures for e-mail be communicated to all patients who desire to communicate electronically.

(3) The policies and procedures for e-mail be applied to facsimile communications, where appropriate.

(4) The policies and procedures for e-mail be applied to text and electronic messaging using a secure communication platform, where appropriate.

ABOUT NORCAL GROUP

The NORCAL Group of companies provide medical professional liability insurance, risk management solutions and provider wellness resources to physicians, healthcare extenders, medical groups, hospitals, community clinics, and allied healthcare facilities throughout the country. NORCAL Group includes NORCAL Mutual Insurance Company and its affiliated insurance companies. Please visit norcal-group.com/companies for more information.

Revised: August 2018

NORCAL GROUP®

BEST PRACTICES: RISK MANAGEMENT RESOURCE

COMMUNICATION: PATIENT PORTALS

Patient portals are secure online websites providing patients with 24-hour access to their health information, including lab and test results, clinical visit summaries, appointments, immunizations, and medications. Through the patient portal, patients can update their contact information, request prescription refills, schedule appointments, make payments, fill out questionnaires and forms, view educational materials and exchange secure messages with their health care team. These websites are hosted on secure encrypted servers and patients can access them anytime using a secure username and password.

Medical Professional Liability Risks

Patient portals, if set up properly and monitored, can help with efficiencies in practice, improve the quality of communication with patients, and increase patient engagement. However, patient portals also present a number of risks, including:

- Patients opting to use the portal in an emergency situation resulting in a bad or unexpected outcome
- Security and confidentiality related challenges with patients using unsecure devices outside of the practice network
- Lack of proper documentation in the medical record.

Patient satisfaction and understanding must also be considered. Physicians and health care providers should be mindful of possible pitfalls that might be encountered when patients have immediate access to their information.

Patient Engagement

Patient portals can increase patient engagement so long as patients use them. Patients who are otherwise engaged in their healthcare may avoid using patient portals because they have limited computer skills. One way to reach patients who may be struggling with the technical aspects of engaging through a portal is to offer training sessions to show them how to get online, establish an account and navigate the portal to retrieve information and contact the practice. Teaching your patients how to use your portal is also a good way for you to learn about its user-friendliness. If using your portal frustrates you and/or your staff, you may need to make some usability changes.

The management of patients, particularly those with chronic illness, can be enhanced by use of a portal. Patients can securely message simple questions to clinicians thereby reducing “phone tag” (that can result in delays and miscommunication), unnecessarily long phone conversations, and unnecessary trips to the doctor. With some portals, patients can provide information in the form of photos, videos, or wireless monitoring devices that the physician can then review and provide additional instruction or feedback to the patient. Beginning in 2019, these asynchronous remote evaluations and virtual check-ins may be reimbursable by Medicare. Reminders from the practice also help increase patient engagement and thereby may improve the patient’s overall health. Be mindful that while a patient

portal is a great way to save time and engage patients, it is a supplement to, not a substitute for, telephone discussions or face-to-face encounters with patients.

Patient Expectations/Portal Guidelines

In order to manage patient expectations, guidelines for the use of the patient portal should be communicated to the patient, verbally and in writing. The guidelines should include information for the patients on approximate turn-around time for responses to email messages. If the portal only allows access to certain information, the guidelines must be clear in explaining that only limited information will be available. A patient may be able to perform the following tasks:

- Check their appointment schedules and request an appointment
- View lab and test results and basic patient information such as BMI, BP, and weight
- Examine medical and billing statements
- Request prescription refills
- Complete new patient intake forms, registration information and yearly paperwork
- Complete ongoing assessment forms
- Correspond with medical personnel via encrypted email services
- Update personal information

It is important to relay to the patients that the use of a portal is inappropriate for medical emergencies, highly sensitive subjects, complex medical conditions or other situations in which an in-person examination or detailed follow-up is necessary.

Privacy and Security Issues

Physicians should not use the portal for clinical communications without establishing appropriate safeguards to ensure confidentiality is not breached. All physicians who transmit any protected health information electronically must comply with the HIPAA Privacy and Security Rules as well as state privacy and security laws. Portals should be hosted on a secure connection and access should only be via an encrypted, password-protected log-in site.

HIPAA requires physicians to protect patient information. This obligation extends to patient information maintained in, or available through, a patient portal. This does not mean that the physicians must police to whom the patients grant access, but it does require the physician establish safeguards to prevent unauthorized access to the patient's information. Because portals by their nature are sending information to patients, who are most likely using unsecure devices outside of the practice network, there will always be a risk with such technology.

It is particularly important to maintain the privacy of sensitive information such as mental health and substance abuse treatment records and HIV related information. Care should be taken to determine what records to make available on patient portals and that appropriate authorizations for release are in place.

Educate patients on ways to use the portal to help maintain privacy and security of information, e.g., do not give your username and password to others, use only a personal or secure device to log in, do not store or save your password on any computer or mobile device, and log off when a session is complete.

Parent Access to Patient Portals

When a child reaches the age of 13 (or whatever age state law designates), parental access to the child's medical information should be limited pursuant to federal and state privacy laws. At that point, the practice needs to protect the confidentiality of the adolescent patient's sensitive condition treatment information in the patient portal, unless the child has authorized parental access to the protected information. Parents start with full access until their child reaches adolescence, then they lose access to sensitive information, and finally they lose access to all of their child's medical information when the child reaches the age of 18. The parent can request adult proxy access which would need to be approved by the adult child.

The ease with which this can be done is dependent on the portal's filter capacities. If a portal system can limit the data accessible to parents, the practice will need to determine which information to limit pursuant to federal and state privacy laws and how to manage the shift of diminishing/expanding access from parent to child as the child matures. Sensitive information (e.g. labs related to pregnancy, sexually transmitted illnesses, genetic results, select confidential appointments and potentially sensitive problems and medications) can be tagged and sent only to the adolescent patient's account.

Documentation

All email exchanges with patients should be maintained in the patients' medical records. Such documentation is important to defend against professional liability claims or payor audits, because it can be used to support or justify the medical necessity or appropriateness of the care provided or of subsequent care. Some patient portals may not seamlessly integrate email communication with the practice's electronic health records system. Practices should ensure there is a way to capture this communication via the patient portal into the medical record.

Risk Management Recommendations

Patient Engagement/Training

- Offer patients training sessions to show them how to get access and navigate the portal.
- Monitor and facilitate appropriate usability changes.
- Establish guidelines to manage patient expectations as to how and what information will be accessible.
- Educate patients on what is appropriate use of the portal, i.e., non-urgent concerns only, no emergencies.

Patient Expectations/Portal Guidelines

- Establish a policy that details how frequently practitioners must check their inboxes and the process by which results are then communicated to the various parties who need to see them.
- Use the portal only as a secondary means to communicate lab and procedure results.
- Keep patient-physician communications professional and straightforward. If the communication is complex or if a patient requires repeated information, answers or details, insist on an appointment for a face-to-face encounter.
- Develop consistent processes around the use of the patient portal (e.g., who will sign patients up, who will receive any email communications posted to the portal site, how often email messages will be checked, etc.).
- Consider installing an agreement on the patient portal site which will require the patient to read the terms and conditions of using the site and sign off that they read and agree to them. Maintain this document in the patient's medical record.
- Consider providing large font alerts on the portal emails or login that remind patients of the limitations of using the site (e.g., length of time until response, no emergency conditions, etc.).

Privacy and Security

- Comply with HIPAA Privacy and Security Rules and state privacy and security laws.
- Ensure emails can be securely sent to and received from patients.
- Encrypt all electronic transfers of confidential medical information and have security policies in place.
- Use firewalls and password protection to ensure that only designated users can gain access to confidential medical information and communications.

Parent Access to Patient Portals

- Work closely with IT personnel and attorneys to safeguard confidential adolescent healthcare information in patient portals.
- Ensure parents and adolescents understand the services and information that will be available to them through the patient portal.
- Have a system in place to authenticate parents/guardians during the portal registration process.

Documentation

- Document all email messages in the patient's medical record.
- Retain email failure messages (rather than deleting them) when transmissions are unsuccessful, and then use alternative means to contact the patient. Email fails for a variety of reasons (wrong addresses, system blocks, various technical issues, etc.). Retaining failure messages may help in the defense of a claim if there is some question as to why message transmission was unsuccessful.

Revised: May 2019

Additional Resources

- Patient portal tools are available in the Health Literacy Universal Precautions Toolkit, 2nd Edition. Available at: www.ahrq.gov/professionals/quality-patient-safety/quality-resources/tools/literacy-toolkit/healthlittoolkit2.html (accessed 3/27/19).
- The U.S. Department of Health & Human Services Agency for Healthcare Research and Quality (AHRQ) provides a Portal Feedback Form at: www.ahrq.gov/professionals/quality-patient-safety/quality-resources/tools/literacy-toolkit/healthlittoolkit2-tool17b.html (accessed 3/27/19).
- Bourgeois FC, et al. Whose Personal Control? Creating Private, Personally Controlled Health Records for Pediatric and Adolescent Patients *J.AM.Med. Inform. Assoc. 2008;15(6):737-743*. Available at: http://jamia.oxfordjournals.org/content/15/6/737.long (accessed 3/27/19).
- Meaningful Use Case Studies: Patient Portal Benefits Patient Care and Provider Workflow (2011, Winter). Available at: https://www.healthit.gov/case-study/patient-portal-benefits-patient-care-and-provider-workflow
- What is a Patient Portal? Available at: www.healthit.gov/providers-professionals/faqs/what-patient-portal (accessed 3/27/19)
- Patient Portal Identity Proofing and Authentication Guidance from the Healthcare Information and Management Systems Society (HIMSS) Identity Management Task Force. Available at: www.himss.org/sites/himssorg/files/Patient_Portal_Identity_Proofing_and_Authentication_Final.pdf (accessed 3/27/19)
- Get Paid for Using the Patient Portal. Available at: https://www.medicaleconomics.com/technology/get-paid-using-patient-portal?rememberme=1&elq_mid=5998&elq_cid=103592&GUID=31C4113D-F1EB-4DDC-9D89-D9EF4AB82471 (accessed 3/27/19)

Revised: May 2019

***CLAIMS Rx:* FEBRUARY 2018**

TELEMEDICINE RISK MANAGEMENT — THE FUTURE IS NOW

CLAIMS Rx
CLINICAL & RISK MANAGEMENT PERSPECTIVES
NORCAL GROUP®
FEBRUARY 2018

Telemedicine Risk Management — The Future is Now

Telemedicine Risk Management — The Future is Now

CME INFORMATION

Sponsored by:
The NORCAL Group of companies includes NORCAL Mutual Insurance Company, along with its subsidiary companies Medicus Insurance Company, FD Insurance Company, NORCAL Specialty Insurance Company and its affiliate Preferred Physicians Medical RRG.

NORCAL Mutual Insurance Company is accredited by the Accreditation Council for Continuing Medical Education to provide continuing medical education for physicians.

METHOD AND MEDIUM

To obtain CME credit, read the enduring material article then log in to your online account to take the CME quiz, or download the free MyNORCAL® app, to get your certificate. The MyNORCAL app is available now for iOS and Android and has all of the same CME materials available in MyACCOUNT and automatically syncs your CME activity with your other devices.

Access your account online:

NORCAL Group:
norcal-group.com

Create an account
MyACCOUNT and the MyNORCAL app require a NORCAL Group login. Call Risk Management Department for an activation code/Client ID 855.882.3412.

Please complete and submit the online quiz by the expiration date indicated below:

Original Release Date:
January 15, 2018

Expiration Date:
February 1, 2020

No Available CME Credits

LEARNING OBJECTIVES

By reviewing medical professional liability claims and/or emerging topics in healthcare risk management, this enduring material series will support your ability to:

- Assess your practice for risk exposures.
- Apply risk management best practices that increase patient safety and reduce medical professional liability claims.

TARGET AUDIENCE

Physicians, healthcare staff and administrators.

CREDIT DESIGNATION STATEMENT

NORCAL Mutual Insurance Company designates this enduring material for a maximum of *1 AMA PRA Category 1 Credit™*. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

DISCLOSURE POLICY

As an ACCME accredited provider, NORCAL Mutual Insurance Company requires planners, reviewers or authors who influence or control the content of a CME activity to disclose financial relationships (of any amount) they have had with commercial interests associated with this CME activity during the year preceding publication of the content. Any identified conflicts of interest are resolved prior to the commencement of the activity.

DISCLOSURES

Individuals involved in the planning, reviewing or execution of this activity have indicated they have no relevant financial relationships to disclose.

EDITOR

Mary-Lynn Ryan, JD
Risk Management Specialist, NORCAL Mutual

CONTENT ADVISORS

Sandra L. Beretta, MD
Chair, NORCAL Mutual, FD Insurance and Medicus

Patricia A. Dailey, MD
Director, NORCAL Mutual, FD Insurance and Medicus

Rebecca J. Patchin, MD
Director, NORCAL Mutual, FD Insurance and Medicus

William G. Hoffman, MD
Family Practice Content Advisor

Dustin Shaver
Vice President, Risk Management, NORCAL Mutual

Neil Simons
Vice President, Product Development, NORCAL Mutual

Paula Snyder, RN, CPHRM
Regional Manager, Risk Management, NORCAL Mutual

Katey L. Bonderud
Claims Specialist, NORCAL Mutual

Kellie N. Sorenson, JD
Sr. Counsel, NORCAL Mutual

PLANNER

Shirley Armenta
CME Program Lead, NORCAL Mutual

INTRODUCTION

Telemedicine is gaining momentum. Third-party payment for telemedicine is increasing, state medical boards are working to make practicing in multiple states less onerous for physicians, and patients are demanding it.

The implications for patient safety and risk management are still uncertain. At the current time, the number of NORCAL liability claims directly related to the use of telemedicine is low. In claims that involve telemedicine, the technology has been a peripheral issue that has little effect on the cause of injury. However, as the number of telemedicine encounters increases, patient injuries and malpractice claims directly associated with it will likely increase.[1]

This month's publication primarily draws case study fact patterns from policyholders' calls to the Risk Management Department. Over the past few years, policyholder calls to the Risk Management Department about telemedicine have been concentrated in a few different areas:

- Physicians who want to join a virtual care network (e.g., American Well, MDLive, Doctor on Demand and Teladoc)
- Physicians who want to treat established patients who have moved out of state (or country)
- Physicians who want to offer telemedicine services to existing patients in the same venue
- Practices/groups that want to engage a specialist to provide telemedicine consultations to their patients (e.g., teledermatology, teleneurology), or a specialist who wants to provide virtual consults or second opinions
- Physicians who want to know if they can use a particular technology/platform to provide medical advice (e.g., Skype, FaceTime, Grand Rounds, HealthTap)

These queries align with potential risk exposure issues, including:

- **Recordkeeping:** Virtual care vendor patient recordkeeping protocols can impact contracting physicians' ability to comply with recordkeeping laws, patient safety standards and risk management recommendations.
- **Physician-Patient Relationship:** When the physician-patient relationship is created and ends may be ambiguous in virtual care arrangements.
- **Quality of Care:** Telehealth platforms may make providing quality care complicated. Clinicians need to determine when the patient needs to be seen in person, whether a diagnosis can be made without touching or smelling the patient and whether the patient has the capacity to engage via telemedicine.
- **Informed Consent:** In addition to the risks, benefits and alternatives associated with the treatment being contemplated, the patient should be educated about the risks, benefits and alternatives associated with telemedicine.
- **Technology:** The technology used on both ends of the encounter needs to be adequate for the medical care contemplated. Internet connectivity, power outages, bandwidth issues and inadequate technology support during a consult can cause diagnosis delays, errors and patient dissatisfaction.
- **HIPAA:** Telehealth technology needs to maintain the privacy and security of patient health information (PHI).
- **Licensure:** Clinicians need to be licensed in the state in which the patient is receiving care, as well as in the state in which the physician is physically located.
- **Contracts:** Telemedicine company contracts may impact quality of care, compliance with healthcare laws and defense of liability claims.

It is important for individual physicians to understand how the telehealth platform affects their ability to provide quality care and manage risk. There can be tremendous pressure on physicians to achieve excellent patient ratings and attract a new generation of patients that wants fast, efficient and "no hassle" care by offering virtual care. Vendors may pitch telemedicine as an easy way to increase revenue, reduce burnout, increase patient access and improve patient well-being. However, physicians must not be swept up in the tide of excitement without a risk management and patient safety plan in place.

Defining Telemedicine

Telemedicine and telehealth are often used interchangeably. In the broadest sense, they both refer to the use of technology to deliver healthcare at a distance.[i] According to the American Telemedicine Association, telehealth is a delivery tool or system, while telemedicine is healthcare that utilizes telecommunications technologies.[ii] Telemedicine can be thought of as any type of patient care that involves telecommunication, including videoconferencing, transmission of still images and other data, e-health (patient portals, websites), m-health (mobile healthcare service), remote monitoring and medical call centers.[ii]

Resources

i. Health and Public Policy Committee of the American College of Physicians, Daniel H, Sulmasy LS. Policy Recommendations to Guide the Use of Telemedicine in Primary Care Settings: An American College of Physicians Position Paper. *Ann Intern Med.* 2015;163(10)787-789. Available at: ***annals.org/article.aspx?articleid=2434625*** (accessed 1/10/2018).

ii. ATA Standards and Guidelines Committee. Core Operational Guidelines for Telehealth Services Involving Provider-Patient Interactions. 2014. Available at: ***www.uwyo.edu/wind/_files/docs/wytn-doc/toolkit-docs/ata_core_provider.pdf*** (accessed 1/10/2018).

Risk Issues Associated with Synchronous Virtual Care

Virtual care is not inherently riskier than seeing a patient in the office. However, limitations with the current state of technology and the existence of a third-party virtual care vendor serving as a conduit between clinician and patient can increase patient safety and liability risk. Physicians can become involved in virtual care through different pathways. Many healthcare systems that offer virtual visits contract with one of the major virtual care companies and then brand the virtual care platform under their own name. Patients in the healthcare system frequently have access to physicians in their own healthcare system, but may also have access to the virtual care company's panel of physicians.[2] Small private practices that have historically lacked the technical infrastructure for virtual care are also starting to have opportunities to provide virtual care to their patients with the major virtual care companies.[2,3] Finally, physicians can choose to join a virtual care physician panel as independent contractors. This option is often presented to physicians as a way to make extra income or as an alternative way to practice medicine.

The NORCAL Risk Management Department has received numerous calls from policyholders who are considering joining the physician panel of a synchronous virtual care provider (e.g., American Well, MDLive, Doctor on Demand and Teladoc). Physicians calling were ready to enter into virtual care agreements without realizing the unique patient safety and liability risks associated with this new care delivery methodology. The following case studies are drawn from those calls.

Virtual Care Recordkeeping

In the virtual care arrangement contemplated in the following case, the physician did not know how he could comply with medical record retention, security, access, and release regulations, or whether he would have access to a complete copy of all records in the event of a lawsuit.

CASE ONE

Issue: The physician had not thoroughly considered the unique recordkeeping issues associated with virtual care.

The physician's group was planning to contract with a second-opinion virtual care company. According to the physician, the vendor described the process as follows: patients filled out an intake form, uploaded their medical records and requested a second opinion. The virtual care company then chose a physician from the company panel of contracted physicians. If the chosen physician agreed to provide the second opinion, the patient and physician were connected and communication took place via the company's virtual care platform. The physician would provide a written opinion that was uploaded to the system, where the patient could access it.

DISCUSSION — VIRTUAL CARE RECORDKEEPING

Physicians own the physical medical record, while patients own the information in the record (for the most part). The era of electronic medical records — by adding a vendor to the equation — has changed the thinking around ownership and control of medical records and patient information. Telehealth will further change the dialogue, because the telehealth platform vendor controls so much of the transaction between the physician and patient. Virtual care platform designers may not consider medical record documentation and accessibility by physicians a priority; however, physicians who use telehealth modalities must document, retain and provide patient access in a manner consistent with current laws and regulations governing healthcare recordkeeping. It will be important for physicians contemplating virtual care to carefully review contracts to ensure their appropriate access to patient records.

RISK MANAGEMENT **RECOMMENDATIONS**

VIRTUAL CARE RECORDKEEPING

Because a virtual care encounter may be conducted entirely through a third-party, it is important to know how to comply with various recordkeeping regulations and patient record access expectations. Consider the following recommendations:[2]

- Have a clear mechanism to access, supplement and amend patient information.
- Know how the patient obtains a copy of the virtual care consultation record.
- Ensure the patient's ability to access a copy of the record is consistent with state and federal law.
- Obtain assurances that a complete legal record of the virtual care consultation will be made available to you if it is needed to defend care in a malpractice action or regulatory matter, such as a board of medicine inquiry.
- Establish who on the patient's healthcare team should receive reports of the encounter.

RISK MANAGEMENT **RECOMMENDATIONS**

TELEMEDICINE ENCOUNTER DOCUMENTATION

Documenting a virtual care encounter requires additional details. If an unexpected outcome occurs as a result of a telemedicine encounter, it is important to know the cause, for both risk management and quality improvement. Without clear documentation, it can be difficult to determine the cause of an unanticipated outcome. In addition to clinical information, documentation should include:[4,5,6]

- The exact time when you were contacted to provide a consult, the time that you were connected to the patient, and, if it is an emergency, the time that you recommended treatment and when the treatment was provided.
- Your location and the location of the patient.
- The names and contact information for everyone involved in the encounter, including the person who requested the examination and the telepresenter (a person in the remote location assisting with the consultation), if there is one.
- Patient authentication: Will you be able to ensure you are examining and prescribing for the correct person? Some ways to authenticate the patient include:
  - Asking the patient to hold up a driver's license to the camera and comparing the information on the identification card to the information provided by the patient.
  - Running an insurance eligibility check, confirming the patient's name, address, date of birth and Social Security number.
  - If the patient has been seen before, asking a series of questions on prior medical history to determine if the patient responses match what is in the medical records.
- The informed consent process and confirmation, including that the patient agrees to and understands that you may determine telemedicine may not be appropriate for the diagnosis and treatment of his or her condition.
- Who provided observations associated with a component of a physical examination; for example, if the telepresenter assessed the strength or tone of the patient, add to the documentation "per telepresenter."
- Ancillary reports that contributed to the examination — if the reports are not available in the file, identify the clinician who read the report to you.
- Any technical issues that interfered with, delayed or complicated the telemedicine encounter, for example, poor internet connectivity or signal quality, camera or device malfunction, telepresenter unavailability, patient inability to manage technical aspects of the exam, or peripheral device unavailability.

Patients Recording or Posting Virtual Care Encounters

Whether patients are allowed to record a virtual care encounter can be analogized to patients creating sound or video recordings with their smartphones during in-person examinations. There are pros and cons associated with allowing patients to record healthcare encounters. On the pro side, patients can play the recording when they forget the details of treatment recommendations or the risks, benefits and alternatives associated with proposed treatment. However, the posting of an examination to social media is an entirely different matter in which the cons will most likely outweigh the pros, since it is difficult to determine how posting the visit to social media would enhance the quality of care. Another concern is that the recording could be used in future litigation against the clinician, and that the recording could be altered to favor the plaintiff.

Whether a patient is legally permitted to record a patient encounter (video and/or audio) depends primarily on state wiretapping/eavesdropping laws, which designate whether all parties or just one party must consent to the recording of a conversation. For example, in one-party-consent states, a patient could record an examination without the physician's knowledge or consent. In the other states, recordings without the consent of the physician would be illegal. Currently, 39 of the 50 states and Washington, D.C. are one-party-consent states. The remaining 11 states are all-party-consent states.[iii] However, there may be other state laws that also affect whether recording a telemedicine encounter would be legal. For example, in Vermont, which is a one-party consent state, telemedicine law prohibits recording telemedicine encounters either by the physician or the patient.[iv] Consequently, it is important to understand the state laws affecting wiretapping/eavesdropping and telemedicine encounter recordings when creating patient recording policies. Information about state laws on recording can be accessed at ***www.mwl-law.com/wp-content/uploads/2013/03/laws-on-recording-conversations-chart.pdf*** (accessed 12/1/2017).

The bottom line is: Patients may record and post their virtual care encounters regardless of whether a physician consents to it. Surreptitious recording can't be controlled, but lack of a physician's consent to the recording may affect whether the recording would be admissible as evidence in future litigation. Physicians who do not want to be recorded should develop clearly written policies for consultation recordings and the appropriate response to recording that occurs covertly. If a patient is resistant, offer a summary of the visit, discharge information sheet, educational pamphlets or tools, and/or remind patients to take notes during the encounter and summarize these points with them at the end of the encounter. It is important to clearly document your refusal to consent to the recording.

Physicians affiliated with third-party virtual care vendors who want to make virtual care recordings available to patients must additionally determine whether the recording is allowed by the vendor. If legal or contractual issues do not prohibit recording, it will be important to coordinate and store the various streams of patient data and recordings, and determine how and to what extent this data will be shared and how privacy will be protected. If virtual care recordings are shared with patients, consider entering into an agreement with the patient that limits sharing all or portions of the recording with the general public (e.g., on social media).

Resources

iii. Glyn Elwyn, Paul James Barr, Mary Castaldo. Can Patients Make Recordings of Medical Encounters? What Does the Law Say?. *JAMA*. 2017;318(6):513–514.

iv. Lacktman NM, Ferrante TB. Vermont's New Telemedicine Law Expands Insurance Coverage, Bans Recording. 2017. Healthcare Law Today. Available at: ***www.healthcarelawtoday.com/2017/07/19/vermonts-new-telemedicine-law-expands-insurance-coverage-bans-recording/*** (accessed 12/4/2017).

The Beginning and End of the Virtual Patient-Physician Relationship

In virtual care, the starting point of the physician-patient relationship may be difficult to determine. In either traditional or virtual healthcare, the relationship is established when the physician agrees to treat the patient and the patient agrees to be treated.[7] With virtual care, the telemedicine vendor can play a significant role in the creation of the patient-physician relationship. For example, the virtual care company may match the patient to the physician, or the patient may choose the physician from a selection provided by the company. When the vendor is in the middleman role, it can delay the communication of physician or patient agreement to enter into a treatment relationship. There also may be ambiguity over when the relationship ends, which can expose the physician to allegations of abandonment.

In the following case study, the physician asking for advice about joining a virtual care company as a panel physician had not considered the following issues:

- What expectations will patients have for the physician-patient relationship?
  - Is the limited nature of the relationship described/agreed to by both parties?
  - Is there any expectation by the patient for an ongoing relationship beyond the virtual visit?
- Who is responsible if a patient in need of services selects a physician, but the vendor fails to promptly connect patient and physician, causing a delay in treatment or diagnosis?

CASE TWO

Issue: The physician had not considered unique physician-patient relationship issues associated with virtual care.

A family practice physician wanted to contract with a virtual care company. The process for providing a virtual consultation was described to her as follows: She would indicate her availability to conduct virtual visits through the virtual care platform. Her profile would only be made available to patients located in her state who were in need of basic family medicine acute illness care. When a patient chose her, she would be notified through the platform. She would then be given access to information the patient had entered into his or her profile and the patient and physician would be connected virtually through the platform. The consultation would take place using the patient's and physician's webcams.

DISCUSSION

Although these issues are not settled, it could be argued that the physician-patient relationship begins when the patient chooses the physician from the online panel, particularly if the patient has a reasonable expectation of the relationship beginning at that point, based on the information provided to the patient by the vendor. The physician may have little control over lag time between the patient requesting the consultation and the vendor notifying the physician of the patient request. Some virtual care physician contracts include a waiver of liability. Consequently, if the company causes a delay that results in a patient injury, the physician may be held responsible for negligent delay of treatment that was out of his or her control.

Another unsettled issue is physician-patient relationship termination. If the patient believes he or she has a continuing relationship with the virtual care physician, but the virtual care platform does not support a continuing physician-patient relationship, the physician could be accused of abandoning the patient. Finally, physicians should consider how to handle assignment of virtual care patients whose healthcare needs require in-person consultation or exceed the virtual care physician's scope of practice.

RISK MANAGEMENT **RECOMMENDATIONS**

Consider the following recommendations:

- Ask the virtual care vendor about the time frame from patient request to physician notification, and consider whether you are willing to accept the risks associated with any anticipated delays.
- Understand and confirm or adjust the patient's expectations for his or her relationship with you.
  - If the expectation is for only one virtual encounter with no continuing relationship, obtain consent from the patient prior to the examination.
- Obtain virtual care vendor patient information to determine what the vendor is offering patients.
- Ensure there is an appropriate method for referring patients who need in-person care, or treatment by a specialist that terminates the physician-patient relationship between you and the referred patient.
- Ensure your ability to follow-up on patient compliance with recommendations and your ability to follow-up with the patient to ensure the condition has resolved.
- Understand vendor expectations of your availability and response time. If you do not want to be available 24/7, it is important to ensure you are in control of your schedule.

Patient Selection

Patient selection for virtual care is extremely important in managing risk and ensuring patient safety. For example, writing a prescription for Viagra® or diagnosing pink eye in a toddler via webcam is fairly straightforward, but consulting with a suicidal teenager in a rural area, or with a patient with an unreliable internet connection, or with a patient for whom managing the technology will be challenging involves an entirely different risk/benefit analysis when determining whether telemedicine is an appropriate option. Oftentimes, receiving unsupervised telehealth services requires the patient to take an active and cooperative role in the consultation. Consequently, part of the patient selection process should be assessing the patient's ability to engage in a telehealth encounter without help. Another important consideration will be the probability of the patient requiring emergency services and how quickly he or she can access them. Geographically isolated patients, who stand to gain significantly from telemedicine, often have the poorest infrastructure, resources and capabilities to receive it.[6]

RISK MANAGEMENT **RECOMMENDATIONS**

Consider the following recommendations:[6]

- Ensure the patient has the organizational and cognitive capacity to receive telehealth services.
- Ensure the patient has the technology and connectivity necessary to be adequately examined.
  - The patient may only have access to a cellphone or a computer lacking the bandwidth necessary or connectivity required by the telehealth platform.
- Ensure the patient's condition can be appropriately examined via available telehealth equipment. For example:
  - If you are asked to do an atypical lesion assessment, can you see the lesion clearly enough to make a diagnosis?
  - If you are asked to assess a patient for dizziness, can the camera angle accommodate an appropriate gait assessment?
- Have a patient health emergency protocol.
  - Particularly for behavioral health patients, it's important to know how to get crisis intervention or police involved.

Informed Consent

In addition to informing a patient about the risks, benefits and alternatives associated with a proposed treatment, some states require the patient to also be educated about the risks, benefits and alternatives associated with telemedicine.[8]

RISK MANAGEMENT **RECOMMENDATIONS**

Ensuring the patient understands the limitations and benefits of telemedicine is a good idea, even if the law doesn't require it. Consider the following recommendations:[6]

- In addition to the risks, benefits and alternatives associated with treatment, include in the telemedicine informed consent
  - Consultation structure and timing
  - Triggers for discontinuing the consultation and referring the patient to in-person care
  - Protocols for contacting you following the consultation
  - Patient medical record access, correction, etc., in compliance with HIPAA and any local patient information laws
  - Confidentiality and the limits of confidentiality when communicating via an electronic medium
  - Reassurances that reasonable precautions are being taken to ensure privacy, security of PHI and HIPAA compliance, but it is the responsibility of the patient to ensure a private environment on their end of the virtual consultation to the extent that it is important to the patient
  - Emergency plan
  - Potential for technical failure
  - Care coordination and specialist referral policies
- Provide consent information in language that can be easily understood by the patient, particularly information that refers to technical issues like encryption or the potential for technical failure.
- If the telemedicine platform being used has the consent for telemedicine built into the process, make sure that the elements noted above are addressed.
- Confirm that local laws allow electronic signatures on the consent form.
- Document the consent process in the medical record.

Professionalism

Virtual care encounters require a different communication approach than an office visit. Some physicians may appear perfectly natural to patients who see them on their computer screens and may be able to seamlessly move back and forth between live and virtual patient care. Other physicians' body language or preoccupation with technology may give the impression of a lack of empathy or incompetence. Physicians who treat a virtual health

> Patients notice when professionalism is lacking.

consult too much like a telephone consult, or who fail to set the appropriate stage in their telemedicine office may also make a poor impression. Patients notice when professionalism is lacking. For example, in the comments section of a virtual care website, a patient complained that the physician appeared to be in an office with family

and company in another room who kept passing in the hallway behind him. Another patient was upset that her physician appeared to be reading something from the internet while she was explaining her symptoms.[9] NORCAL Risk Managers have fielded questions from policyholders that raise similar concerns. For example, an intensivist who worked for a tele-ICU company called to ask if he could continue monitoring patients from his hotel room while he was vacationing with his family. Another caller planned to take calls in his car while he and his wife commuted to and from work. Although telemedicine is often seen as a way for physicians to consult with patients more conveniently, maintaining a professional virtual care environment is an important consideration.

RISK MANAGEMENT **RECOMMENDATIONS**

Professionalism should be the same for office and virtual visits. Consider the following recommendations:[6]

- Be comfortable with the telemedicine technology you are using and have access to technical assistance when needed.
- If legal or contractual issues do not prohibit recording, review recordings of your telemedicine consults and determine whether there are aspects of your "on-screen" presence that could be changed to enhance the patient's experience.
- Provide virtual consultations from an environment that is comparable to a professional patient consultation setting.
  - Choose a simple background, without distracting images or objects.
  - Close the door to your office during virtual consultations.
  - Avoid conducting virtual consultations in public places.
  - Take measures to reduce the potential for interruptions during periods while you are doing virtual care.
- Set up your camera and encourage the patient to set up his or her camera in a way that facilitates seeing each other's faces.
- Place your camera on a stable platform in order to transmit a steady image.
- Appropriately light yourself and your surroundings.

Virtual Care Production Quality Resources

With registration, the American Telemedicine Association (ATA) provides guidance on improving quality during a virtual care encounter. For example, the ATA articles, "Let there be Light: A Quick Guide to Telemedicine Lighting," and "A Concise Guide for Telemedicine Practitioners Human Factors: Quick Guide Eye Contact," can both be accessed through the ATA website at: ***www.americantelemed.org/home*** (accessed 12/1/2017).

Quality of Medicine

In general, the quality of telemedicine should be at least equivalent to in-person healthcare for a particular patient presentation. Various issues should be considered when determining whether a patient can be appropriately treated in a virtual manner. Even minor medical complaints, like upper respiratory infection or sore throat, may require hands-on evaluation. For example, one virtual care provider was asked to provide a hand examination for a patient who had throbbing pain in her index and middle finger of her right hand. She described no other symptoms. Her acrylic nails were elaborately decorated for the holiday season. It was only after observing an erythematous and inflamed perionychial area on the left index finger, that the physician got the patient to admit that her nails were emitting a foul odor. She was then able to diagnose abscesses under the nail beds of the right hand. This would require removal of the elaborate acrylic nails, which the patient was trying to avoid. Had the physician been examining this patient in person, the odor of the infection would have made diagnosis relatively simple.

Technology on either end of the consultation may prohibit quality care. Even if the technology meets the standards necessary, inadequate training can create the basis for a malpractice claim. Additionally, inability to obtain information, either through past medical records or ordered labs, studies or consults, may impact a physician's ability to provide treatment consistent with the standard of care. Finally, quality assessment can be difficult if the telemedicine vendor does not allow access to patient complaints and satisfaction surveys. These are all issues that should be considered when considering whether telemedicine is appropriate for a particular patient.

RISK MANAGEMENT **RECOMMENDATIONS**

Consider the following recommendations:[6,10]

- Ensure the patient can be adequately assessed without information normally obtained during an office visit. For example:
  - Does the diagnosis and treatment recommendation require temperature, pulse, blood pressure, throat swab, ear drum examination, palpation, urine sample, strength assessment, reflexes, etc.?
    - Do not be tempted to guess about appropriate treatment if information that would usually be gathered in person is unavailable.
    - Be explicit with a patient who needs to follow up with an in-person clinician and explain the risks of failing to do so.
- Ensure additional patient records can be obtained if necessary for reaching a diagnosis and proposing appropriate treatment.
- Consider how studies, labs or referrals will be accomplished.
  - Determine whether the patient has mobility and is able to comply with referral recommendations.
- Be familiar with the patient's prescription and medication dispensation options.
- Ensure a method to report and coordinate telemedicine consultations with the patient's primary care physician.
- Refer to guidelines to determine whether telemedicine is appropriate in a particular situation or with a particular patient.

Telemedicine Guidelines

Various organizations have published guidelines to assist physicians in the provision of quality telemedicine. For example, the ATA has published "Core Operational Guidelines for Telehealth Services Involving Provider-Patient Interactions." The ATA also has published guidelines for various telemedicine specialty practices, including guidelines for telepathology, teleICU, teledermatology, telemental health and telerehabilitation, which can be accessed through the ATA website at: ***www.americantelemed.org/home*** (accessed 12/1/2017). In addition to the ATA, various medical specialty societies also have published clinical practice guidelines related to telemedicine, including:

- American College of Radiology, "White Paper on Teleradiology Practice"
  Available at: ***www.jacr.org/article/S1546-1440(13)00185-3/fulltext*** (accessed 12/1/2017)
- American Academy of Dermatology, "Teledermatology Toolkit"
  Available at: ***www.aad.org/practicecenter/managing-a-practice/teledermatology*** (accessed 12/1/2017)
- American Academy of Pediatrics, "Telemedicine: Pediatric Applications"
  Available at: ***pediatrics.aappublications.org/content/136/1/e293*** (accessed 12/1/2017)
- American Academy of Neurology, "Resources on Teleneurology"
  Available at: ***www.aan.com/practice/telemedicine/*** (accessed 12/1/2017)

Privacy and Confidentiality

Many forms of interactive audio-visual technology (IAVT) (e.g., Skype, FaceTime) are readily available, inexpensive and provide an opportunity to videoconference via computer, tablet or smartphone. Unfortunately, many popular IAVT tools were not designed for doctor-patient interactions, and can compromise your obligation as a covered entity to comply with HIPAA. IAVT companies may encrypt information that travels through their platforms, but some do not sign business associate agreements, do not provide audit trails, do not ensure security of backup files and do not offer notification in the event of a breach or a security incident. IAVT services that do not perform these functions jeopardize a covered entity's HIPAA compliance and would therefore not be appropriate for providing telehealth services.[11]

RISK MANAGEMENT **RECOMMENDATIONS**

Consider the following recommendations:[6]

- Ensure your telemedicine platform/software/mobile device app secures all data transmissions with point-to-point encryption that meets recognized government standards.
  - More information on encryption standards is available at: ***www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html*** (accessed 12/4/2017).
- Ensure IAVT software is not set to allow outside access to teleconsultation with patients. For example, some platforms may default to create a video "chat room" that allows other users of the platform to enter at will.
- Determine whether videoconference transmission data is inadvertently stored on computer hard drives or smartphones. If so, protect storage security with disk encryption, remote wipe functions and pre-boot authentication. A better strategy is not storing PHI on portable devices.
- Take appropriate precautions to keep others from hearing or seeing PHI (e.g., close the office door; do not conduct telemedicine in public).
  - Ask the patient to do the same.

Licensure and Choice of Law

Obtaining appropriate licensure should be a major consideration for any physician contemplating the practice of telemedicine across state lines. Consulting with patients in distant states without proper licensure may be "practicing medicine without a license," which can have harsh penalties, including criminal prosecution, civil litigation or administrative action. Some states require full licensure while others provide a special limited license through reciprocity. Recent efforts to simplify physician licensing across state lines have been somewhat successful. For example, the Federation of State Medical Boards (FSMB) Physician Licensure Compact provides an expedited licensing pathway for physicians who wish to be licensed in numerous states. More information about the compact is available at: ***www.licenseportability.org*** (accessed 12/2/2017).

In addition to ensuring appropriate licensure, clinicians should also consider the healthcare laws applicable in the patient's location. Standards of care and informed consent laws vary from state to state and may be more or less favorable to clinicians in the event of a medical liability claim. For example, tort reform measures might not apply when a patient is located in a state without them. Additionally, mandatory reporting and related ethical requirements, such as duty to notify, are tied to the jurisdiction where the patient is receiving services.[6]

State medical associations, medical boards and other healthcare organizations provide state-specific telemedicine law summaries. The ATA's "State Telemedicine Gaps Analysis: Physician Practice Standards & Licensure," which is available at: ***www.americantelemed.org/policy-page/state-telemedicine-gaps-reports#*** (accessed 12/2/2017), compares the telemedicine laws in all 50 states. The Center for Connected Health Policy has an interactive US map available at: ***www.cchpca.org/state-laws-and-reimbursement-policies*** (accessed 12/2/2017), which details telemedicine law and policies by state.

Technology

Technology is a major aspect of telehealth that impacts most risk management and patient safety recommendations in some way. Consider the following recommendations:[6,12]

- Establish technological standards for providing telehealth services.
  - Match the technology to the complexity and needs of the situation. For example, a surgeon who is performing robotic surgery from a remote location will have different bandwidth, image resolution and uptime requirements, etc., than a therapist conducting a behavioral health session.
- When using a personal computer, use professional- grade or high-quality cameras and audio equipment at both ends, when necessary.
- Use up-to-date telehealth software and services that will support HIPAA compliance.
- Have a backup plan in place for technology failures (e.g., internet connectivity, power outage and bandwidth issues can be addressed with back-up generators, redundant equipment and other clinicians on-call who can step in if necessary).
- Have a process in place for physicians and patients to report technical insufficiencies (e.g., poor resolution of images, transmission delays, malfunctioning equipment, etc.).
  - Communicate the plan to the patient prior to beginning the consultation, including termination of the session, if technical difficulties become insurmountable.
- Regularly test equipment and connectivity to ensure functionality.
- Use the most reliable connection method possible to access the internet (i.e., use wired connections when possible, and use videoconference software that will adapt to changing bandwidth environments without losing the connection).
- Ensure all members of the telehealth team are complying with technology policies.

Contracts with Telemedicine Vendors

Contracts between telemedicine vendors and physicians may cover many of the issues already addressed in this article, including patient access to medical records, HIPAA compliance, obtaining patient consent, responsibility for technology functionality, paying for telecommunication connection and tech support, credentialing, referrals and indemnification for liability.

> Physicians should not assume that a telemedicine contract takes into account a physician's duty to comply with various healthcare laws, medical ethical standards, patient safety guidelines or professional liability coverage arrangements.

Indemnification language in a contract can shift liability to a physician signatory, even though a patient injury was caused by a telemedicine company. Additionally, the contract's definition of confidential information may be too broad to allow compliance with various laws and guidelines. Finally, verbal promises made to physicians by the company or vendor that conflict with language in the contract will most likely be difficult, if not impossible, to enforce.[6]

RISK MANAGEMENT **RECOMMENDATIONS**

Consider the following recommendations:[13]

- Carefully review all telehealth contracts and strongly consider having a healthcare attorney provide a review.
- Do not agree to a term in a contract if you do not understand the effect it will have on you, your practice or your business.
- Do not ignore an indemnity clause and assume it can be resolved at a future date. In general, it is more difficult to negotiate the terms of a contract after it has been signed.
  - Have an attorney review any contract containing the terms "indemnity," "hold harmless" or anything similar. (An indemnity clause does not have to include the terms "indemnity" or "hold harmless" to shift indemnification to you.)
- Review any liability policies for exclusionary language that may apply to any contract being considered.
- Determine how reimbursement will be managed and ensure it is compliant.

Remote Patient Monitoring

The use of remote patient monitoring by physicians and healthcare entities continues to increase.[14] Remote patient monitoring is using digital technology to collect health data from a patient in one location and electronically transmit that information to a clinician in a different location for assessment. Patient data such as vital signs, weight, blood pressure, blood sugar, blood oxygen levels, heart rate and electrocardiogram can be transmitted from hospitals to monitoring centers such as teleICU units, or from a patient's home to a hospital or primary care unit. Patients can be remotely monitored from home using a variety of different devices. For example, the University of Pittsburgh Medical Center (UPMC) provides congestive heart failure patients with kits containing a pulse oximeter, blood pressure cuff, weight scale and a 4G tablet that uploads data to UPMC nurses who monitor the data.[15]

The following case, which is based on a NORCAL closed claim, involves a different remote patient monitoring scenario. In the following case, the obstetrician on call was monitoring patients using an iPhone app that allowed her to review laboring patient fetal heart monitor (FHM) tracings remotely. Reviewing the case in retrospect, the ability to review the FHM tracings online seemed to lull the physician into a false sense of security about fetal well-being.

CASE THREE

Allegation: The on-call OB, who was watching the patient's fetal monitor tracings on her cellphone app, negligently delayed delivery.

At midnight, an OB nurse called the on-call OB and asked her to come in to examine a high-risk patient and update the care plan. The OB brought up the FHM tracings on her smartphone, and informed the nurse they were not concerning to her. She told the nurse that she would continue to monitor the tracings from her home. She then updated the electronic health record (EHR) from her home computer, noting category 2 tracings and no fetal distress.

By 2:30 a.m., when the OB arrived at the hospital, the FHM tracings were showing repetitive decelerations and the biophysical profile was 2/8. A C-section was called at 3:00 a.m. and started at 3:50 a.m. The infant was delivered with APGARs of 0/0 and could not be revived. Placental pathology showed placental abruption. The mother filed a wrongful death lawsuit against the OB.

DISCUSSION

OB experts who reviewed this case could not support the delay in delivery. They believed the FHM tracings started to look concerning at 1:30 a.m. and were ominous by 2:00 a.m. According to one expert, a jury wouldn't be impressed by the OB's capacity to monitor from home. They would focus on her failure to present to the hospital after the nurse expressed her concern about fetal well-being. Another issue that arose during litigation was the patient's perception that she was being ignored by the OB. The nurse had advised the patient that the physician was monitoring her from home, but the patient considered the off-site monitoring inferior and unsatisfactory. Whether the remote monitoring app inaccurately represented the FHM tracings could not be established.

RISK MANAGEMENT **RECOMMENDATIONS**

Consider the following recommendations:[14,16]

- Be appropriately responsive to the nurse or other patient attendant who is directly observing a patient whom you are remotely monitoring.
- Be sensitive to potential differences in the accuracy of the data generated by remote monitoring devices (e.g., how does the stethoscope plugged into the patient's home computer compare to a stethoscope in person?).
- Regularly ensure the remote monitoring device/software is functioning appropriately.
- Understand the extent of your responsibility for reviewing remote data — will you be responsible for noticing that the patient is having an adverse event at 3:00 a.m., when your practice is to review overnight data at 8:00 a.m. the following morning?
- Have a system for recognizing when patient data is indicating a downward trend.
- Identify patients for whom remote monitoring will be most beneficial (e.g., patients with chronic disease that are most likely to be readmitted to the hospital). Remote monitoring for every patient who requests it may not be appropriate.
- Take into account the potential for patient dissatisfaction with remote monitoring when the patient expects bedside or in-person evaluation, and adequately explain how it works and why it is an appropriate alternative to in-person evaluation.

Clinician Adjustment to New Telehealth Modalities

There may be a period of adjustment while telepresenters/generalists adjust to their new role as conduits of a more specialized or complex practice. In the following case, a rural hospital started using a teleneurology "telestroke robot" when neurologists were not available for consultation. The negligence allegations were not associated with the teleneurology, per se, but rather with the ED physician's and hospitalist's failure to utilize the technology to diagnose the patient's stroke in a timely manner, when it could have been treated. Consider how the following outcome may have been different if the ED physician and hospitalist had been more familiar with the teleneurology policies and protocols.

CASE FOUR

Allegation: The ED physician should have obtained a teleneurology consultation.

At 8:00 p.m., a 25-year-old man arrived by ambulance to the ED. He was obtunded, could not speak and was not responsive. His wife described him as otherwise healthy before he had lost consciousness, although he had been complaining of a headache for the past week. The ED physician considered stroke in her differential, but her index of suspicion for stroke was not high enough to trigger a stroke alarm, which she understood was the requirement for telestroke robot utilization. Therefore, the ED physician ordered a battery of tests and studies, which revealed no obvious reason for the patient's nearly comatose status. She decided to have the patient admitted for further testing. The hospitalist who admitted the patient ordered a neurology consult for the following day when a neurologist would be rounding on patients.

The following day, the neurologist who examined the patient concluded he had suffered a stroke. By this time, the patient's brain damage was extensive. The patient filed a lawsuit against the hospital, ED physician and hospitalist alleging he should have immediately received a teleneurology consultation and, had this been done, his stroke would have been diagnosed, tPA and/or other interventions would have been undertaken and his outcome would have been significantly better.

DISCUSSION

The American Academy of Neurology supports teleneurology as an effective tool for rapid evaluation of patients in isolated and urban areas with too few available neurology specialists. Particularly when stroke is in the differential, teleneurology consultation can significantly reduce the risk of patient injury when a neurologist is not available.[17] In this case, experts believed the ED physician needed to immediately seek consultation from a neurologist when she was unable to determine the etiology of the patient's neurological status. She could have done this using the telestroke robot, but she misunderstood the policy for using teleneurology, assuming it was only to be used to determine whether to administer tPA.

The hospital's policy for using the teleneurology system did not limit use of the teleneurology system to suspected stroke patients; however, the policy was somewhat unclear, as it consistently referred to the "telestroke robot" and "telestroke policy." Consequently, although experts believed the ED physician was personally liable for her failure

to act, the hospital shared responsibility for the poor outcome because the policies and procedures were not effective. Experts believed hospital administrators had a duty to ensure the teleneurology system was being used appropriately before it was made widely available to patients.

RISK MANAGEMENT **RECOMMENDATIONS**

Hospital administrators in this case had no idea that their telestroke robot policies were unclear until it came up in litigation. Consider the following recommendations:

Clinicians and Telepresenters

- Understand the appropriate use of telemedicine in your workplace.
- Stay abreast of telemedicine upgrades and changes in your workplace.
- Comply with telemedicine policies and protocols when appropriate.
  - If some aspect of a policy or protocol is unclear, seek clarification.
- Take advantage of telemedicine training resources and request additional training when necessary.
- Resist being pulled outside of the scope of your license or specialty by telemedicine policies or protocols.

Administrators

- Before rolling out a new telemedicine program, ensure clinicians understand how and when to use telemedicine.
  - Train clinicians on the telemedicine modalities and the policies and protocols for its use.
  - Ensure the wording of telemedicine policies and protocols is not misleading or ambiguous.
- Define general guidelines for telemedicine-appropriate conditions and complaints, but then refine the guidelines as practice indicates.
  - Ensure telemedicine modalities are being utilized appropriately.
- Update telemedicine policies and procedures as technology is updated.

CONCLUSION

Telemedicine laws, technology and guidelines continue to develop and change, which will inevitably result in questions about how to provide telemedicine in a manner that complies with state and federal laws, ethical guidelines and patient safety standards. Understanding and mastering telemedicine-specific patient safety and liability risk issues will be important as telemedicine becomes more ubiquitous in the healthcare arena. With all of the excitement over new technologies and opportunities, it can be difficult to remember that telemedicine, at its core, is simply a means to providing healthcare. Clinicians must be able to comply with the standard of care, and if that is impossible because the physician and patient are in different places, then the patient consultation should take place in person. The strategies and suggestions introduced in this article are presented to help clinicians determine when telemedicine is appropriate and ease the adjustment to this new methodology for practicing medicine.

ENDNOTES

The NORCAL documents referenced in this article, along with many other Risk Management Resource documents and past editions of the *Claims Rx*, are available in the Risk Solutions area of MyACCOUNT, or by policyholder request at 855.882.3412.

1. Ksiazek MC. Telemedicine — Are There Increased Risks With Virtual Doctor Visits? *Nat Law Rev.* 2017. Available at: ***www.natlawreview.com/article/telemedicine-are-there-increased-risks-virtual-doctor-visits*** (accessed 12/5/2017).
2. Terry K. The Key to Making Virtual Visits a Digital Success. *Med Econ.* 2017. Available at: ***medicaleconomics.modernmedicine.com/medical-economics/news/key-making-virtual-visits-digital-success*** (accessed 12/5/2017).
3. Loeb S. How Does Health Tap Make Money? *Vatornews.* 2017. Available at: ***vator.tv/news/2017-03-03-how-does-healthtap-make-money#rvERgo0MTzHJFOJH.99*** (accessed 12/5/2017).
4. Govindarajan, RR, et al. Developing an outline for teleneurology curriculum: AAN Telemedicine Work Group recommendations. *Neurology.* 2017;89(9):951-959.
5. Goedert J. Telemedicine Consults Require Care in Confirming Patient Identity. *Health Data Manage.* 2017. Available at: ***www.healthdatamanagement.com/news/telemedicine-consults-require-care-in-confirming-patient-identity*** (accessed 12/5/2017).
6. American Telemedicine Association. Practice Guidelines for Video-Based Online Mental Health Services. 2013. Available at: ***www.integration.samhsa.gov/operations-administration/practice-guidelines-for-video-based-online-mental-health-services_ATA_5_29_13.pdf*** (accessed 12/5/2017).
7. Kentucky Board of Medicine. Board Opinion Regarding the Use of Telemedicine Technologies in the Practice of Medicine. 2014. Available at: ***kbml.ky.gov/board/Documents/Board%20Opinion%20regarding%20The%20Use%20of%20Telemedicine%20Technologies%20in%20the%20Practice%20of%20Medicine.pdf*** (accessed 12/5/2017).
8. Lacktman NM. Joint Commission Introduces New Accreditation Standards for Telehealth Services. *Health Care Law Today.* 2017. Available at: ***www.healthcarelawtoday.com/2017/09/12/joint-commission-introduces-new-accreditation-standards-for-telehealth-services/*** (accessed 12/5/2017).
9. Amwell. Reviews. Available at: ***www.trustpilot.com/review/amwell.com*** (accessed 12/5/2017).
10. State Medical Boards' Appropriate Regulation of Telemedicine (SMART) Workgroup. Federation of State Medical Boards Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine. 2014. Available at: ***www.fsmb.org/Media/Default/PDF/FSMB/Advocacy/FSMB_Telemedicine_Policy.pdf*** (accessed 12/5/2017).
11. Greve P. Telemedicine Law and Liability: 2015. *Willis Towers Watson Wire.* Available at: ***blog.willis.com/2015/10/telemedicine-law-and-liability-2015/*** (accessed 12/5/2017).
12. Valenti MS. True North|The 24/7 Connected Patient. 2017. Available at: ***thesextantgroup.com/247-connected-patient/*** (accessed 12/5/2017).

1. Armer WD. Indemnification in Healthcare Contracts: Concepts, Coverage and Clauses. Presented at: Dallas Bar Association-Health Law Section Meeting; November 16, 2016.
2. Irfan A. Virtual Care Trend Watch. *Telemedicine Magazine.* 2017. Available at: ***www.telemedmag.com/article/virtual-care-trend-watch/*** (accessed 12/5/2017).
3. University of Pittsburgh Schools of the Health Sciences. Remote Monitoring Telemedicine. 2017. Available at: ***www.upmc.com/healthcare-professionals/physicians/telemedicine/services/Pages/remote-monitoring.aspx*** (accessed 12/5/2017).
4. Chesanow N. Do Virtual Patient Visits Increase Your Risk of Being Sued? *Medscape.* 2014. Available at: ***www.medscape.com/viewarticle/833254_6*** (accessed 12/5/2017).
5. McCormick T. Teleneurology: Why It Works for Rural Hospitals. *Telehealth and Medicine Today.* 2017:(2)5. Available at: https://telehealthandmedicinetoday.com/index.php/journal/article/view/72 (accessed 3/18/2019)

CLAIMS Rx

CME ACTIVITY

ACCME ACCREDITED WITH COMMENDATION

Telemedicine Risk Management — The Future Is Now

DON'T FORGET TO DOWNLOAD THE FREE

MyNORCAL® CME APP

to complete your CME credits for this article (Details on page 4).

*Search '**MyNORCAL**' in the App Store or Google Play*

Download on the App Store | ANDROID APP ON Google play

NORCAL GROUP® 844.4NORCAL (844.466.7225) | norcal-group.com

NORCAL GROUP®

***CLAIMS Rx:* OCTOBER 2018**

HIPAA DATA BREACH PREVENTION AND MANAGEMENT

CLAIMS Rx
CLINICAL & RISK MANAGEMENT PERSPECTIVES
NORCAL GROUP®
OCTOBER 2018

HIPAA Data Breach Prevention and Management

The healthcare industry experiences more data breaches (confirmed data disclosures) than any other industry in the United States, accounting for more than 24% of all breaches.[1] In 2017, healthcare data breaches compromised more than 5 million healthcare records[2] and cost providers an average of $380 per record[3] — more than any other industry and 69% greater than the overall average.

HIPAA Data Breach Prevention and Management

CME INFORMATION

Sponsored by:
The NORCAL Group of companies includes NORCAL Mutual Insurance Company, along with its subsidiary companies Medicus Insurance Company, FD Insurance Company, NORCAL Specialty Insurance Company and its affiliate Preferred Physicians Medical RRG.

NORCAL Mutual Insurance Company is accredited by the Accreditation Council for Continuing Medical Education to provide continuing medical education for physicians.

METHOD AND MEDIUM

To obtain CME credit, read the enduring material article then log in to your online account to take the CME quiz, or download the free MyNORCAL® app, to get your certificate. The MyNORCAL app is available now for iOS and Android and has all of the same CME materials available in MyACCOUNT and automatically syncs your CME activity with your other devices.

Access your account online:

NORCAL Group:
norcal-group.com

Create an account
MyACCOUNT and the MyNORCAL app require a NORCAL login. Call Risk Management Department for an activation code/Client ID 855.882.3412.

Please complete and submit the online quiz by the expiration date indicated below:

Original Release Date:
December 15, 2015

Reviewed and re-released:
October 15, 2018

Expiration Date:
October 1, 2020

LEARNING OBJECTIVES

By reviewing medical professional liability claims and/or emerging topics in healthcare risk management, this enduring material series will support your ability to:

- Assess your practice for risk exposures.
- Apply risk management best practices that increase patient safety and reduce medical professional liability claims.

TARGET AUDIENCE

All healthcare providers.

CREDIT DESIGNATION STATEMENT

NORCAL Mutual Insurance Company designates this enduring material for a maximum of *1 AMA PRA Category 1 Credit™*. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

DISCLOSURE POLICY

As an ACCME accredited provider, NORCAL Mutual Insurance Company requires planners, reviewers or authors who influence or control the content of a CME activity to disclose financial relationships (of any amount) they have had with commercial interests associated with this CME activity during the year preceding publication of the content. Any identified conflicts of interest are resolved prior to the commencement of the activity.

DISCLOSURES

Individuals involved in the planning, reviewing or execution of this activity have indicated they have no relevant financial relationships to disclose.

EDITOR

Mary-Lynn Ryan, JD
Risk Management Specialist,
NORCAL Group

CONTENT ADVISORS

Jaan E. Sidorov, MD
Chair, NORCAL Mutual and Medicus
Vice Chair, PMSLIC

Patricia A. Dailey, MD
Vice Chair of the Board,
NORCAL Mutual and Medicus

Rebecca J. Patchin, MD
Director, NORCAL Mutual and Medicus

William G. Hoffman, MD
Family Practice Content Advisor

Dustin Shaver
Vice President, Risk Management,
NORCAL Group

Neil Simons
Vice President, Product Development,
NORCAL Group

Paula Snyder, RN, CPHRM
Regional Manager, Risk Management,
NORCAL Group

John Resetar
Claims Specialist, NORCAL Group

Andrea Koehler, JD
Counsel, NORCAL Group

PLANNER

Shirley Armenta
CME Program Lead, NORCAL Group

INTRODUCTION

The healthcare industry experiences more data breaches (confirmed data disclosures) than any other industry in the United States, accounting for more than 24% of all breaches.[1] In 2017, healthcare data breaches compromised more than 5 million healthcare records[2] and cost providers an average of $380 per record[3] — more than any other industry and 69% greater than the overall average.

More than half of all healthcare cybersecurity incidents (regardless of whether data was compromised) are the unintentional result of employee error[1] or occur in various preventable ways, including:[4]

- Loss or theft of computers, storage devices or smartphones containing patient information from cars, offices, briefcases, employees' homes, hotel rooms, etc.
- Incorrectly addressed email containing patient information
- Inappropriately accessed electronic patient records by unauthorized employees
- Hacked servers

Even the most innocent mistake, if it leads to a data breach, can result in costly and disruptive incident investigation, patient notification expenses and significant fines and corrective action requirements.

An analysis of NORCAL Group data breach closed claims shows that inadvertent, unauthorized release of medical records or patient information is the most frequent reason for a data breach claim. Theft or loss of portable electronic devices like laptops, flash drives and smartphones is the second most frequent reason. NORCAL has also seen a marked increase in the past two years in incidents involving hacking, malware, and viruses, which (together) is now tied with theft/loss of portable devices as the second most common reason for a data breach claim.

Whether a privacy or security incident is a HIPAA breach depends on the nature of the PHI and the circumstances of the use or disclosure.

This article uses case studies based on NORCAL Mutual HIPAA data breach closed claims. The case studies introduce strategies to help reduce the risk of HIPAA data breach and to appropriately respond to a breach when it happens. While the following discussion is not meant to be a comprehensive overview of compliance with the HIPAA Privacy and Security Rules, compliance with the rules should prevent many security breaches. Guidance and additional information on the HIPAA Security Rule, and on medical record security, access and release are available to all NORCAL Mutual insureds through their MyACCOUNT, or by contacting a NORCAL Risk Management Specialist at 855.822.3412.

NORCAL Mutual Information and Network Security Insurance Coverage

NORCAL Mutual provides Information and Network Security Insurance coverage as part of the Health Care Professional (HCP) policy at no additional cost, which includes coverage for:

- Regulatory privacy proceedings, including HIPAA proceedings
- Patient notification and credit monitoring
- Electronic data recovery and replacement

More information about the Information and Network Security Insurance Coverage can be obtained by contacting the NORCAL Mutual customer service team or your underwriter at 844-4-NORCAL.

HIPAA Terms

According to the HIPAA statute, **Protected Health Information (PHI)** is individually identifiable health information created or received by a healthcare provider regarding the physical or mental health of any individual that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. **Electronic protected health information (ePHI)** is PHI that is created, stored, transmitted, or received electronically. The focus of this article is ePHI, although a HIPAA data breach can occur with paper records. When patient data or patient healthcare information is referenced in this article, it refers to ePHI.

A covered entity is a health plan, healthcare clearinghouse or healthcare provider who transmits any health information in electronic form for qualifying transactions. Guidance on how to determine whether a healthcare provider is a covered entity is available at: ***cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html*** (accessed 5/31/2018).

Resource
Cornell Law School, Legal Information Institute. U.S. Code of Federal Regulations. 45 CFR §160.103. Available at: ***law.cornell.edu/cfr/text/45/160.103*** (accessed 5/31/2018).

What is a HIPAA Data Breach?

In general, a HIPAA data breach is an impermissible use or disclosure that compromises the security or privacy of PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity can show there is a low probability the PHI has been compromised based on a risk assessment of at least the following four factors:[5]

1. The nature and extent of the PHI involved in the use or disclosure, including the types of identifiers and the likelihood that PHI could be re-identified (e.g., aggregated PHI vs. complete, intact patient records)

2. The unauthorized person who used the PHI or to whom the disclosure was made (e.g., whether the inadvertent disclosure was made to another covered entity regulated under HIPAA vs. a hacker)

3. The likelihood that any PHI was actually acquired or viewed (e.g., an audit trail shows there has been no access to the databases at risk vs. a stolen laptop with PHI stored on the hard drive where access cannot be determined)

4. The extent to which the risk to the PHI has been mitigated (e.g., encryption keys are promptly changed and network access monitoring shows no access vs. lost device with no opportunity to determine whether access has occurred)

When performing this assessment, a covered entity must address each element separately and then analyze the combined four elements to determine the overall probability that PHI has been compromised. If this assessment indicates there is low likelihood of compromised PHI, then the use or disclosure may not be classified as a HIPAA breach, and notification may not be required. If, on the other hand, the covered entity is unable to overcome the presumption of a breach and show that there is a low likelihood that the PHI was compromised, then breach notification may be required.[5]

HIPAA Data Breach Safe Harbor and Exceptions

Whether a privacy or security incident is a HIPAA breach depends on the nature of the PHI and the circumstances of the use or disclosure. Included in the HIPAA regulations is a critical safe harbor: If an impermissible use or disclosure involves PHI that has been rendered unusable, unreadable, or indecipherable (i.e., encrypted or remotely cleared, purged or destroyed), it does not rise to the level of a breach and, therefore, does not require notification.[5]

If the incident involves unsecured PHI, but the disclosure falls into one of three narrow breach exceptions, notification is similarly not required. According to the HHS website[6]:

> "The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
>
> The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
>
> The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information."[6]

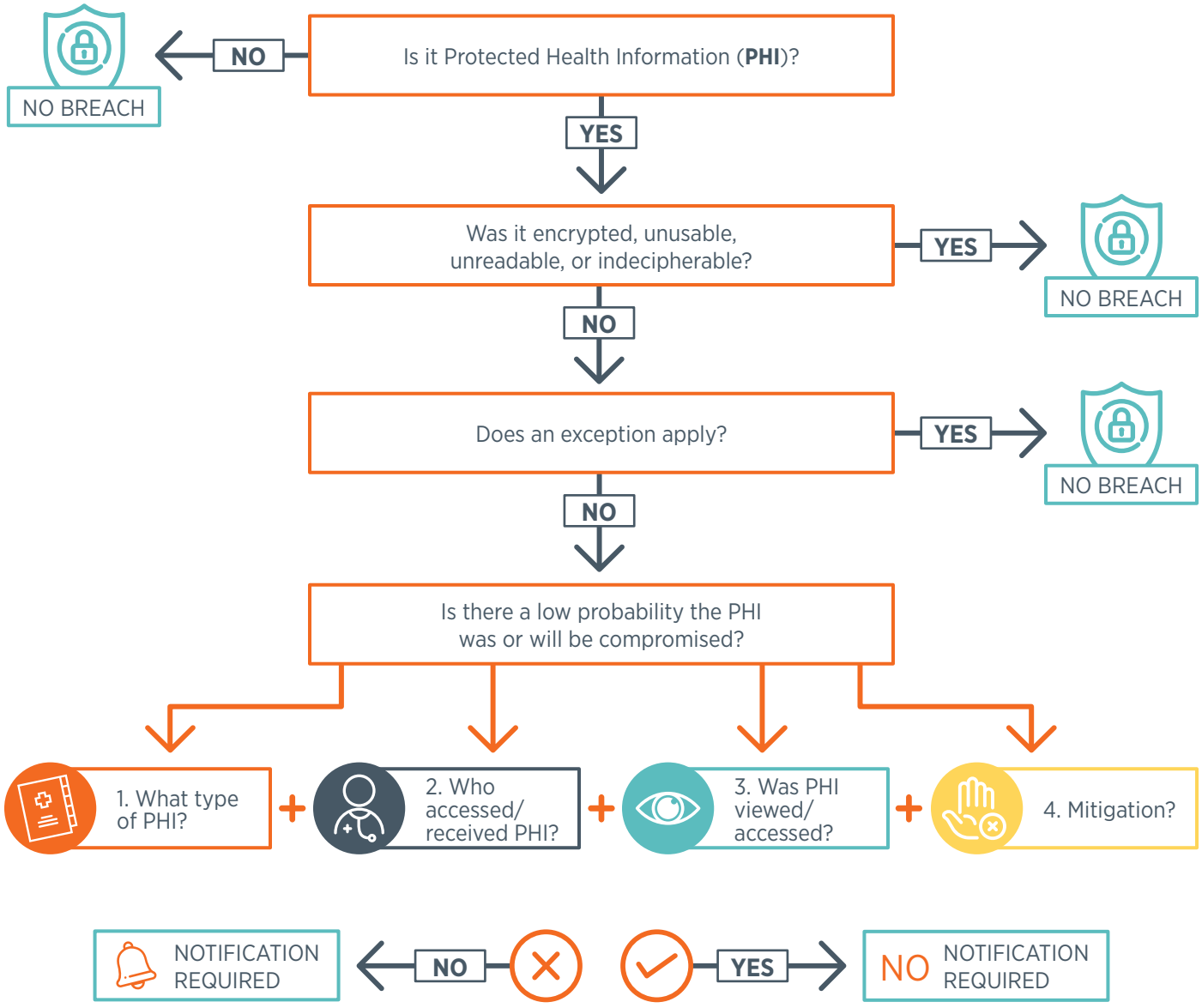
HIPAA Breach Notification

The HIPAA Breach Notification Rule requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information.[6] Covered entities must notify affected individuals, HHS and at times the media about the HIPAA breach. To whom and when notification must occur primarily depends on the number of individuals affected by the breach. If there is a breach of unsecured PHI that affects 500 or more individuals, the covered entity must notify the individuals and HHS without reasonable delay, and no later than 60 days after the covered entity discovers the breach. Once notified, HHS posts the breach on the HHS Office for Civil Rights (OCR) Breach Portal Website, which is available at: ***ocrportal.hhs.gov/ocr/breach/breach_report.jsf*** (accessed 5/31/2018). The OCR is responsible for investigating breach incidents to determine if they were the result of HIPAA violations. OCR investigations may be initiated based on complaints, breach reports, information from other government agencies or reports in the media.

If the breach affects 500 or more individuals in the same jurisdiction or state, the covered entity must also notify the media. If a breach affects fewer than 500 individuals, the covered entity must notify affected individuals without reasonable delay, and no later than 60 days after discovery of the breach, and HHS no later than 60 days after the end of the calendar year in which the breach occurred.[5,6]

HIPAA Breach Analysis Flowchart

The following flowchart outlines how a privacy or security incident is analyzed to determine whether a HIPAA breach has occurred. It forms the basis of the analyses in the case studies in this article.



In addition to federal HIPAA regulations, covered entities may also have to comply with state data breach laws. State laws vary on what triggers a breach notification obligation and the nature of breach notification obligations. This publication focuses on federal data breach notification laws. The Health Information & the Law website has an interactive map that provides links to state health data security and breach notification laws, which is available at: ***healthinfolaw.org/state*** (accessed 5/31/2018).

PHI on Stolen Computers

According to HHS, more than a third of all data breaches to date involved a laptop, desktop, or mobile device.[7] Compare Cases One and Two, and consider how better security practices protected the covered entity in Case Two.

CASE ONE

At a busy family practice office, a medical assistant was tasked with reviewing 100 random patient records for quality purposes. Because she was about to miss her deadline for the project, she downloaded the records onto her laptop so she could work on the project over the weekend. She put her laptop in her car trunk and met friends for dinner on the way home. While she was having dinner, her laptop was stolen. The data on the laptop were not encrypted and there was no password protection.

HIPAA Breach Analysis

Q. Was PHI involved?
A. Yes. Full medical records were being stored on the laptop.

Q. Was the information on the compromised device encrypted, unusable, unreadable, or indecipherable?
A. No.

Q. Does one of the three disclosure exceptions apply?
A. No. Theft of a computer/storage device is not considered an exception.

Q. Is there a low probability that PHI has been compromised? *(Risk Assessment)*

1. Type of PHI: The information was very sensitive and included numerous patient identifiers. There was a high possibility the PHI could be used by an unauthorized recipient in a manner adverse to the patients, or could be used to further the unauthorized recipient's own interests.
2. Who took it/received it: Unknown
3. Ease of access: Whether the medical information was viewed was unknown, but because there was no password protection on the computer, the chance that the PHI could be viewed was high.
4. Mitigation: There was no way to assure the PHI would not be used.

A. The attorney who reviewed this case found that based on the risk assessment the clinic could not demonstrate a low probability that the PHI was compromised; therefore, a breach occurred. The practice was required to comply with the HIPAA breach notification requirements.

CASE TWO

At a community clinic, a nurse practitioner (NP) carried a laptop computer with her, using it to enter patient information into the electronic health record (EHR) as she examined patients. Between patients, she left her laptop at the nurses' station while she went to get a cup of coffee in the break room. When she returned, the laptop was gone. The laptop required a password to sign on. Although the NP accessed patient records from the laptop, no PHI was stored on the device's hard drive. In order to access the patient records, she had to sign on to the EHR system with a unique user name and password. She immediately reported to the office administrator that the laptop had been stolen. The administrator immediately disabled the NP's user account. Although the laptop was never recovered, the administrator monitored the EHR system to determine whether anyone had attempted to sign on with the NP's credentials, and no one had.

HIPAA Breach Analysis

Q. Was PHI involved?
A. Yes. PHI could be accessed from the device, but there was no PHI stored on the device.

Q. Was the information on the compromised device encrypted, unusable, unreadable, or indecipherable?
A. No.

Q. Does one of the three disclosure exceptions apply?
A. No. Theft of a computer/storage device is not an exception.

Q. Is there a low probability that PHI has been compromised? *(Risk Assessment)*

1. Type of PHI: The information was very sensitive and included numerous patient identifiers. There was a high possibility the PHI could be used by an unauthorized recipient in a manner adverse to the patients or could be used to further the unauthorized recipient's own interests.
2. Who took it/received it: Unknown
3. Ease of access: Because the computer was password protected, did not store any PHI and required additional password sign-in to access the EHR, the chance that PHI could be accessed was low.
4. Mitigation: The office administrator moved quickly to disable the NP's user account, which would most likely prohibit the thief from being able to access the community clinic patient records.

A. In this case, the attorney who reviewed the case found that based on the risk assessment the clinic could determine there was a low probability the PHI had been compromised. Therefore, it was determined that notification was not required under the HIPAA breach notification rules.

RISK MANAGEMENT: **LAPTOP THEFT PREVENTION**

The Federal Trade Commission suggests an individual think of his or her computer as cash on the table or an open wallet sitting on the back seat of a car.[8] Consider the following strategies to safeguard laptops:[8,9]

- If a laptop must be left unattended, lock it to something heavy with a laptop security cable.
- Make computers personally identifiable with permanent markings or engravings.
- Install a computer alarm that activates when the computer is moved out of a particular range.
- Install a program that tracks the location of a stolen computer.
- When going through airport security, keep your laptop and phone with you until the last minute, then visually track them and retrieve them immediately.
- When staying in a hotel, lock your laptop in the safe, lock it to something heavy or take it with you.
- Do not leave your laptop in a car.
- Do not use a laptop bag; consider using a bag that hides the fact that there is a laptop in it.
- Encrypt your computer's hard drive.
- Keep your laptop password protected and do not store passwords with, in or on it.
- If you have to put your laptop on the floor, place it between your legs so you remember it.
- Institute "clean desk" policies for employees, requiring secure physical locations for devices both during and outside of standard work hours.

Stolen Smartphones

According to the 2018 Verizon Data Breach Investigations Report (DBIR), physical theft and loss of devices accounts for more than 10% of all data breaches in healthcare. Chances are, a certain number of clinicians and staff who use their smartphones to send and receive PHI will have their phones stolen. For general information on securing smartphones, the FCC Communications Commission offers their FCC Smartphone Security Checker with tips for various brands of phones, available at: ***fcc.gov/smartphone-security*** (accessed 5/31/2018). Clinicians and staff who are contemplating using their cellphones to transmit PHI should consult with IT professionals to determine whether the devices can be appropriately secured for HIPAA compliance.

Resource
Verizon Enterprises. 2018 Data Breach Investigations Report. Available at: ***verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf*** (accessed 5/31/2018).

PHI on a Flash Drive

A data breach doesn't need to be criminal or intentional to be reportable. When a storage device is small, it is sometimes difficult to determine whether the device was lost, misplaced or stolen. However, even if a flash drive is presumably lost, a breach analysis must still be conducted and potentially affected patients must be notified if there is a probability of data compromise.

CASE THREE

A staff member at a large health facility saved the PHI of 600 patients on a flash drive for a diabetes management outreach project. A couple of weeks later, when she returned to the task, she could not find the flash drive. A thorough search of her office did not turn up the missing flash drive, and it was presumed lost.

HIPAA Breach Analysis

Q. Was PHI involved?
A. Yes.

Q. Was the information on the compromised device encrypted, unusable, unreadable, or indecipherable?
A. No. The PHI was not secured.

Q. Does one of the three disclosure exceptions apply?
A. No. Theft, loss or misplacement of a storage device is not an exception.

Q. Is there a low probability that PHI has been compromised? *(Risk Assessment)*

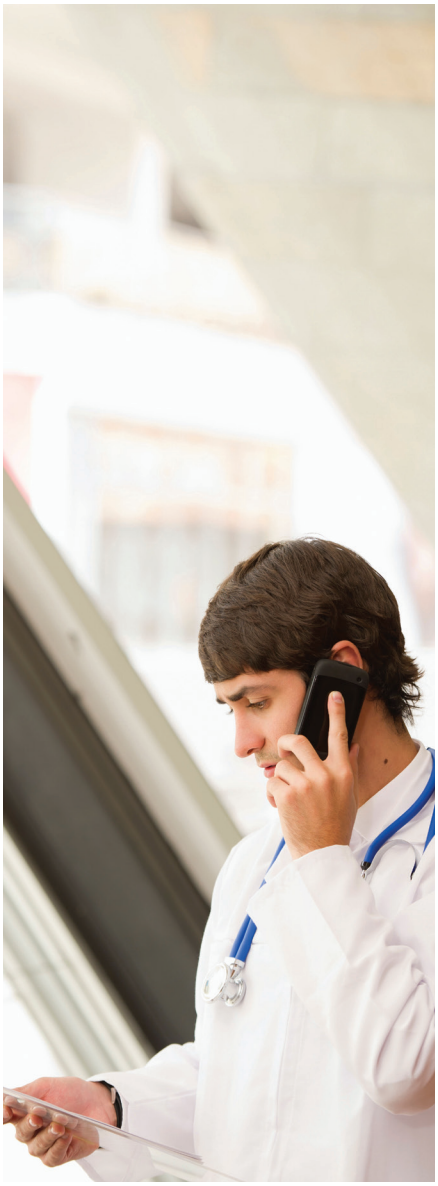
1. Type of PHI: The information was sensitive and included numerous patient identifiers. There was a high possibility the PHI could be used by an unauthorized recipient in a manner adverse to the patients or could be used to further the unauthorized recipient's own interests.
2. Who took it/received it: Unknown
3. Ease of access: Because the PHI on the flash drive was not encrypted or otherwise secured, the chance the PHI could be accessed was high.
4. Mitigation: Nothing could be done to mitigate the potential misuse of the information.

A. The attorney who reviewed this case found that based on the risk assessment the facility could not demonstrate a low probability that the PHI was compromised. Therefore, notification was required under the federal data breach laws. Because the breach involved more than 500 patients in the same state, the breach had to be reported to patients, HHS and prominent media outlets without reasonable delay, and no later than 60 days after discover of the breach.

The notice to the patients had to be written in "plain language" and include:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known
- A description of the types of unsecured PHI that were involved in the breach
- Any steps individuals should take to protect themselves from potential harm resulting from the breach
- A brief description of steps the covered entity is taking to investigate the breach, to mitigate harm to individuals (including providing identity theft protection services for those affected), and to protect against any further breaches
- Contact procedures for individuals to ask questions, including a toll-free telephone number, email address, website or postal address.

Because over 500 patients lived in the same state, the covered entity also had to send major media outlets in that state a notification (i.e., a press release) that included the same information sent to patients. Furthermore, the practice's report to HHS was posted on the OCR Breach Portal. In addition to complying with federal requirements to notify HHS and patients, the covered entity had to follow applicable state regulations. The state where the breach took place had PHI data breach statutes and regulations in place that required an additional notification to the state department of health, which was required on an expedited basis.



RISK MANAGEMENT **RECOMMENDATIONS**

- If your EHR is cloud based, consider accessing the data directly over a secure connection rather than downloading it to another device.
- Carefully consider whether it is necessary to transfer PHI to a flash drive or other portable storage device. Choose a more secure alternative when possible; for example,
  - Download the data directly from the EHR onto a secure device.
  - Transfer the PHI via a secure channel such as secure file transfer protocol (SFTP).
- Encrypt any PHI on storage devices.
- Password protect storage devices.
- Utilize flash drives with remote kill or remote wipe functions.

Mobile Device Policies

Creating mobile device policies can be tricky. Burdensome security policies and strategies that diminish productivity will most likely result in workarounds that defeat security efforts.[i,ii] Additionally, human error and criminal intent can defeat the best-intentioned employee laptop and storage device security strategies. Despite these difficulties, mobile device policies are a necessary part of a comprehensive information security program to prevent HIPAA data breaches. Encryption can secure PHI as it moves though the information stream and into computers and mobile devices. Encrypted PHI is less likely to be compromised if devices are lost, stolen or nefariously accessed. Additionally, there are various technologies available on the market that can dynamically detect and redact PHI and block sensitive information from being downloaded to certain devices.[i]

The HHS ***HealthIT.gov*** website has extensive guidance on using mobile devices in clinical practice. The website includes videos on securing PHI on mobile devices, downloadable posters, presentations and fact sheets to help covered entities comply with HIPAA data security requirements. These resources are available at: ***healthit.gov/resource/your-mobile-device-and-health-information-privacy-and-security*** (accessed 5/31/2018).

Bring Your Own Device (BYOD) Policies

A Bring Your Own Device (BYOD) Policy should be put in place when administrators, clinicians and staff are allowed to use personally owned devices (e.g., laptops, tablets, smartphones) to access, manipulate, use, copy, store or move PHI. Lost and stolen devices are a major source of data security breaches.[iii] The simple act of enabling device security options such as password protection, device encryption, fingerprint or facial authentication, and time-out locks can help prevent HIPAA data breaches by making PHI inaccessible.

Many device users don't even realize when they are exposing PHI to a security breach. For example, various apps don't store content on a device, they store it in the cloud. In many apps, the content is stored in the cloud by default, which requires device users to disable the cloud storage function if they don't want data to be held there. When users don't disable cloud storage, PHI can exist in multiple locations on cloud servers that cannot be controlled by the covered entity that is responsible for the security of the PHI. Covered entities that allow BYOD should develop and implement a policy defining how PHI must be protected, what steps must be taken if a personally owned device that potentially contains PHI is lost or otherwise compromised and the personal consequences of violating the BOYD policy.[ii,iv]

Resources

i Bitglass. 2014 Bitglass Healthcare Breach Report. Available for download from ***pages.bitglass.com/pr-2014-healthcare-breach-report.html*** (accessed 5/31/2018).

ii Pennic J. 68% of Healthcare Data Breaches Due to Device Loss or Theft, Not Hacking. HIT *Consultant.* Available at: ***hitconsultant.net/2014/11/04/healthcare-data-breaches-device-theft-loss/*** (accessed 5/31/2018).

iii Verizon Enterprises. 2018 Data Breach Investigations Report. Available at: ***verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf*** (accessed 5/31/2018).

iv Virtu. HIPAA Email Compliance: 6 Best practices for medical Data Security. Jan 8, 2015. *VirtuBlog.* Available at: ***virtru.com/blog/hipaa-email-compliance/*** (accessed 5/31/2018).

Compromised Email

A common scenario in email security breaches is seen when a billing service sends bills to an incorrect email address. In most practice arrangements, a third-party billing company will have signed a business associate agreement. According to HIPAA, business associates must inform covered entities when they discover a security breach; however, HHS gives covered entities and business associates flexibility in defining, in the business associate agreements, how and when a business associate should notify the covered entity of a potential breach.[10] Consider the following case (please note the following case focuses on the clinic's responsibility to analyze the risk and perform the breach notification, even though the breach was caused by a business entity):

CASE FOUR

A family practice group had a business associate agreement with a billing company. An employee in the billing company sent an email with an attachment that contained patient information for 70 patients to an incorrect email address. Public records indicated the email address was active, but attempts to contact the individual associated with the email address were unsuccessful.

HIPAA Breach Analysis

Q. Was PHI involved?
A. Yes.

Q. Was the information on the compromised device encrypted, unusable, unreadable, or indecipherable?
A. No. The PHI was unsecured.

Q. Does one of the three disclosure exceptions apply?
A. No. Although the transmission of the PHI to the incorrect email address was inadvertent, the PHI was sent to an individual who was not associated with the group or its business associates who could have accessed the PHI.

Q. Is there a low probability that PHI has been compromised? *(Risk Assessment)*

1. Type of PHI: The information in the email was sensitive and included numerous patient identifiers. In the wrong hands, there was a high possibility the PHI could be used in a manner adverse to the patients or could be used to further the unauthorized recipient's own interests.
2. Who took it/received it: The data exposure was inadvertent, but whether the PHI would be further disseminated was unknown because the owner of the email address did not respond to inquiries.
3. Ease of access: The PHI was not encrypted and could be easily accessed.
4. Mitigation: There was nothing the practice could do to mitigate the potential misuse of the PHI.

A. The attorney who reviewed this case found that based on the risk assessment the clinic could not demonstrate a low probability that the PHI was compromised; therefore, a breach occurred. The practice was required to comply with the HIPAA breach notification requirements. Patient notification had to be accomplished within 60 days. However, because the breach involved fewer than 500 patients the group was advised it could maintain a log or other documentation of any other data breaches occurring in that year, and submit all of the breach notifications together not later than 60 days after the end of the calendar year.

RISK MANAGEMENT **RECOMMENDATIONS**

In the foregoing case, the breach was caused by a business associate, but it just as easily could have been caused by an in-house billing department. The HIPAA Security Rule does not prohibit the inclusion of PHI in email, but the HIPAA standards for access control, integrity and transmission security require covered entities and their business associates to have policies and procedures in place that protect the security of PHI in email. If email is not encrypted, HIPAA requires a risk assessment of how the integrity of the PHI will be protected. Consider the following recommendations:[11]

- Consider using the encrypted messaging capabilities in your EHR (if available) to send PHI instead of using general email applications such as Outlook.
- Encrypt email.
- Put a disclaimer on email to mitigate a security breach if PHI is sent an unintended recipient. For example:

  This email message and any attachment(s) transmitted with it are intended only for the use of the recipient(s) named above. This message may contain privileged and confidential information, including patient information protected by federal and state privacy laws. If you are not an intended recipient, you may not review, copy or distribute this message. If you have received this message in error, please notify the sender immediately by reply email and delete the original message.
- Employ interactive software (e.g., a pop-up box) that prevents or warns the sender when he or she is emailing PHI. Remind the sender to double check the email address.
- Give patients the option of receiving unencrypted email only after they had been advised of and consented to the risk of data breach.
  - The HHS website answers questions about email communication with patients at: ***hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html*** (accessed 5/31/2018).
- Include email security requirements in business associate contracts.

Employee Theft, Malicious Data Exfiltration and Voyeurism

Employees access PHI for various illegitimate reasons. Including error and misuse, 71% of all cyber incidents in healthcare have an insider source[1]— the only industry that has more internal sources than external. Although the following case study involves only one patient, the covered entity was required to complete a data breach analysis and notify the patient and HHS.

CASE FIVE

A receptionist at an obstetrics and gynecology group accessed the records of her ex-husband's new girlfriend, who was a patient. The receptionist discovered in the records that the patient had a record of treatment for sexually transmitted diseases (STDs). The receptionist downloaded portions of the patient's record detailing the STD treatment and later anonymously emailed the records to her ex-husband. The ex-husband confronted the patient, who reported the privacy violation to the group. The group's IT department was able to identify the receptionist as the culprit, and she was fired.

HIPAA Breach Analysis

Q. Was PHI involved?
A. Yes.

Q. Was the information on the compromised device encrypted, unusable, unreadable, or indecipherable?
A. No.

Q. Does one of the three disclosure exceptions apply?
A. No.

Q. Is there a low probability that PHI has been compromised?
A. The compromise of PHI was established, and because none of the exceptions applied the attorneys who reviewed this case determined a breach had occurred and notification of the affected patient and the HHS was necessary. The patient had to be informed no later than 60 days after the breach was discovered (although she already knew all about it). Because the breach involved fewer than 500 patients, the group was required to report it to HHS not later than 60 days after the end of the year.

RISK MANAGEMENT **RECOMMENDATIONS**

Comprehensive and effective staff/clinician policies are the backbone of an effective security strategy. However, the best policies can't be successful if employees aren't aware of them or do not follow them. Therefore, covered entities need to train all clinicians and staff on PHI security and breach policies and protocols and consistently enforce violations. Consider the following recommendations:[12,13]

- Provide clinician and staff training initially and then annually on PHI security.
- Ensure clinicians and staff understand PHI security policies and protocols.
- Ensure clinicians and staff understand their responsibilities and roles in protecting PHI security, the various sensitivity levels of information and how PHI should be accessed, stored and transmitted.
- Require staff to sign confidentiality agreements.
- Enforce PHI security policies consistently among clinicians, staff and administrators. (HIPAA requires all covered entities to have sanction policies and procedures in place and to take actions against workforce members who do not comply with them.)
- Inform individuals working with PHI that accessing PHI for reasons not related to their job functions is a violation of state and federal privacy law.
  - Consider using a pop-up box warning users they are accessing PHI and all accesses are being audited (if true).
- Limit clinician and staff access to the data they need to perform their job functions. (E.g., there was no reason for the receptionist in Case Five to have access to patient progress notes.)
- Ensure clinicians and staff are prepared to appropriately respond to a suspected data breach.
- Constantly audit systems to discover improper access.
- Monitor for and resolve inappropriate user ID and password sharing.

Hackers

A review of the data on the OCR Breach Portal indicates that only about 20 percent of healthcare data breaches are the result of hacking, but they involve large numbers of records.[7] Unfortunately, the healthcare industry also has more data breaches than any other industry.[1] There are various reasons for this, some of which we describe below.

Stringent Disclosure Requirements in Healthcare

The healthcare industry is subject to more stringent breach disclosure requirements than are most other industries due to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

High Value of Medical Records

Electronic health records are a more attractive target to criminal hackers due to the greater potential for financial gain and less risk relative to obtaining other types of information.[1] Electronic health records are far more valuable on the black market than credit card information. They are more valuable in part because they contain more information (e.g., health insurance policy information and drug prescription information, which have various uses independently and in combination with the other common information in health records).

Low Risk for Criminals

Additionally, patients are less likely to notice their PHI is being misused than they are to notice unauthorized charges on their credit card, which usually results in closing an account and significantly diminishing the value of the stolen information. Patients can't close their health records and start over. The information can be used indefinitely.[14]

Less Sophisticated Cybersecurity in Healthcare

Finally, healthcare entities are often easier to hack into than financial institutions and retailers because electronic recordkeeping is relatively new to the healthcare industry and fraud is frequently not treated with the same priority as it is in financial or retail institutions. This has resulted in less sophistication in data security tools and strategies used among healthcare providers.[15]

Hackers can strike anywhere. They access PHI through various avenues, including email servers, EHR systems, network servers and portable devices connected to various servers. The HHS website reports hacking incidents affecting numerous healthcare entities, from solo practice physicians to university hospitals to nationwide health insurers. Hackers, when they can be identified, range from disgruntled employees attempting to divert patients to competitors to sophisticated offshore hacking rings that presumably steal health data to sell on the black market.[10]

Just like laptop or cellphone theft, hacking seems inevitable. The most sophisticated perimeter defense (programs to keep hackers out of the system, e.g., firewalls) is unlikely to completely prevent hackers from getting into data systems. Data security experts advocate for increased efforts in deterring hackers from extracting data from systems they have accessed or have attempted to access. One way to accomplish this objective is by applying security controls at various layers, such as implementing intrusion prevention software at the network perimeter, in addition to deploying monitoring software inside the perimeter that is designed to alert on anomalous PHI access attempts. A third layer and example would be applying encryption to all PHI, thus reducing the risk of exposure if other efforts are thwarted and the PHI is extracted.

RISK MANAGEMENT **RECOMMENDATIONS — CYBERSECURITY**

Consider the following recommendations:[1,4,10,16]

- Invest in up-to-date data loss prevention (DLP) technology.
- Train employees on data security practices and awareness.
- Perform suspicious email training exercises to help employees identify potentially nefarious emails.
- Regularly monitor networks and databases for unusual traffic.
- Develop risk assessments and incident response plans for irregular server activity.
  - Consider designating staff to carry out security monitoring.
- Ensure that your sensitive data is backed up regularly in case of a ransomware attack or system failure that causes loss of data.
- Protect your most critical digital assets by segregating them and prioritizing them in your business continuity plan.
- Inoculate yourself by encrypting sensitive data and enabling password protection and remote erasing capabilities on all devices containing sensitive data to secure data in case of device loss or theft.
- Implement email security software that guards against email fraud, impostor email, phishing, malware and spam.
- Enable network and device firewalls.
- Keep all operating systems and software up-to-date with the latest security patches, especially highly targeted software like Microsoft Office apps.

NIST Cybersecurity Practice Guides

The National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) has a wealth of resources targeting specific cybersecurity challenges in the public and private sectors. These practical, user-friendly guides can help your practice facilitate the adoption of standards-based approaches to cybersecurity. The publications with specific applicability to healthcare are:

- 1800-1 Securing Electronic Health Records on Mobile Devices
- 1800-3 Attribute Based Access Control
- 1800-4 Mobile Device Security: Cloud and Hybrid Builds
- 1800-6 Domain Name System-Based Electronic Mail Security
- 1800-8 Securing Wireless Infusion Pumps in Healthcare Delivery Organizations
- 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events

These publications are available at: ***csrc.nist.gov/publications/sp1800*** (accessed 5/31/2018).

Encryption

Failure to adequately safeguard PHI can result in costly and time-consuming forensic investigations to determine whether and to what extent data may have been accessed. PHI encryption is a way to avoid these difficulties. If PHI is appropriately encrypted, there is a low probability that anyone other than the intended party who has the private key will be able to decrypt and ultimately decipher the contents. Using strong encryption may be the most efficient and effective means to avoid HIPAA data breach, as the rule makes clear that impermissible use or disclosure of PHI encrypted pursuant to HIPAA guidelines is not considered a breach.[10,17]

HIPAA defines encryption as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of confidential process or key."[18] Data at rest (i.e., data stored in work stations, laptops, tablets, phones, flash drives, or external hard drives) and data in motion (i.e., data in a non-persistent state that is in transit across the Internet, wireless networks and connections, etc.) are addressed separately in HIPAA encryption guidance.[17] According to the Breach Notification Rule, the proper standards for encrypting data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices, available at ***csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf*** (accessed 10/28/2015).[17] The appropriate standards for encrypting data in motion are consistent with any of the following NIST publications:[19]

- 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations. Available at: ***nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf*** (accessed 5/31/2018)
- 800-77, Guide to IPsec VPNs. Available at: ***csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf*** (accessed 5/31/2018)
- 800-113, Guide to SSL VPNs. Available at: ***csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf*** (accessed 5/31/2018)
- 140-2, Security Requirements for Cryptographic Modules. Available at: ***csrc.nist.gov/groups/STM/cmvp/standards.html*** (accessed 5/31/2018)

RISK MANAGEMENT **STRATEGIES FOR AVOIDING HIPAA DATA BREACH**

Consider the following recommendations:[5,20]

Educate Staff and Clinicians

- Know what state and federal health data security laws require.
- Educate clinicians, staff and administrators on responding to a data security incident.
- Educate clinicians and staff about proper protocol when handling PHI on a mobile device.
  - The HHS HealthIT website has two different computer games created for training healthcare clinicians and staff on HIPAA device security. The games can be accessed at: ***healthit.gov/topic/privacy-security/privacy-security-training-games*** (accessed 5/31/2018).

Assess Data Security Risk

- Perform thorough HIPAA risk assessments on a regular basis.
  - Analyze all sources, systems, movement and storage of PHI.
  - Document the results of the risk assessment.
  - Implement additional safeguards to address any security risks identified.

Mitigate Data Security Risk

- Imagine all of the ways data can be inappropriately accessed, and put up road blocks.
  - Encrypt all PHI.
  - Install software to remotely wipe PHI and disable passwords in case of device loss or theft.
  - Require authentication to access mobile devices, including complex passwords or biometric measures.
  - Encrypt email and text messages.
  - Install software to stop viruses and malware.

Monitor for Security Breach

- Implement a data activity monitoring system to alert IT to potential security threats.
  - The HHS OCR HIPAA Audit Protocol provides guidance for determining monitoring protocols. It is available at: ***hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html*** (accessed 5/31/2018).

Respond to Security Incidents

- Have a documented data security incident response plan in place.
  - Identify who is on the incident response team and what actions they will take to address the incident.
  - Report security incidents to the covered entity's information technology/security department and the NORCAL Mutual Claims Department at 844-4-NORCAL.
  - Notify affected patients and the appropriate regulatory agencies in the manner advised by your attorney.

Every data security incident is unique (despite seemingly similar fact patterns) and federal and state data security breach regulations are constantly evolving and changing. It is important to stay current with breach notification requirements. Because breach notification is time sensitive, immediate action is frequently required. Although HIPAA generally allows 60 days for notifying patients and regulatory agencies about a breach, state law may require shorter notification periods, and determining the breadth of a security incident may involve hiring outside IT professionals, which can be time consuming.

CONCLUSION

The first step in preventing a costly security breach from having an impact on your practice is to take HIPAA compliance seriously. Know the rules and ensure employees, consultants and business associates are all on the same page about PHI security, recognizing and reporting potential security breaches in a timely manner and enforcing data security policies and protocols. Unfortunately, one forgetful or malicious individual can cause a data breach at a practice with comprehensive data security policies, protocols and education programs. Some of the key ways to most effectively avoid data breaches are: adopting widespread encryption, performing comprehensive risk assessments periodically and focusing on appropriate controls with regard to laptops and portable media.

Special thanks to Ross C. D'Emanuele, Partner, Dorsey & Whitney, LLC and Kelly Nicholson, Systems Engineer, Security, NORCAL Group who originally reviewed this article.

ENDNOTES

The NORCAL documents referenced in this article, along with many other Risk Management Resource documents and past editions of the *Claims Rx*, are available in the Risk Solutions area of MyACCOUNT, or by policyholder request at 855.882.3412.

1. Verizon Enterprises. 2018 Data Breach Investigations Report. Available at: ***verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf*** (accessed 5/31/2018).
2. Identity Theft Resource Center. 2017 Annual Data Breach Year-End Review. Available at: ***idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf*** (accessed 5/31/2018).
3. Ponemon Institute. 2017 Cost of Data Breach Study: United States. Available at: ***ponemon.org/library/2017-cost-of-data-breach-study-united-states*** (accessed 5/31/2018).
4. Intel. Grand Theft Data – Data Exfiltration Study: Actors, Tactics, and Detection. 2015. Available at: ***mcafee.com/us/resources/reports/rp-data-exfiltration.pdf*** (accessed 5/31/2018).
5. Office of the National Coordinator for Health Information Technology (ONC). Guide to Privacy and Security of Electronic Health Information. Chapter 7. Breach Notification, HIPAA Enforcement, and Other Laws and Requirements. Available at: ***healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-7.pdf*** (accessed 5/31/2018).
6. HHS. Breach Notification Rule. Available at: ***hhs.gov/hipaa/for-professionals/breach-notification/index.html*** (accessed 5/31/2018).
7. U.S. Department of Health and Human Services Office for Civil Rights (OCR). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Available at: ***ocrportal.hhs.gov/ocr/breach/breach_report.jsf*** (accessed 5/31/2018).
8. Federal Trade Commission, Consumer Information. Laptop Security. Available at: ***consumer.ftc.gov/articles/0015-laptop-security*** (accessed 5/31/2018).
9. Oglesby P. Laptop Anti-Theft: Travel Identity Theft Computer Theft Prevention. updated on Sept 19, 2016. Available at: ***hubpages.com/technology/Laptop-How-to-Protect-Your-Compouter*** (accessed 5/31/2018).
10. Federal Register Volume 78 Number 17, Page 5656 (January 25, 2013). Available at: ***gpo.gov/fdsys/pkg/FR-2013-01-25/html/2013-01073.htm*** (accessed 5/31/2018).
11. SCRYPT Corporation. Email to provider revealed as the reason for recent Atlanta data breach. 18 Aug 2015. ***scrypt.com/blog/email-to-provider-revealed-as-the-reason-for-recent-atlanta-data-breach/*** (accessed 5/31/2018).
12. Paez M, Curley K. Employee-caused data breaches. Wells Fargo White Paper.
13. Raths D. How employee snooping results in HIPAA trouble. *Behavioral Healthcare Magazine.* 5 Dec 2014. Available at: ***behavioral.net/article/how-employee-snooping-results-hipaa-trouble*** (accessed 5/31/2018).
14. Wild D. Experts: Be Prepared for EHR Breaches *Pain Medicine News.* April 2015;20(4). Available at: ***painmedicinenews.com/Commentary/Article/04-15/Experts-Be-Prepared-For-EHR-Breaches/29090*** (accessed 5/31/2018).
15. Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. 24 Sep 2014. Reuters. Available at: ***reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924*** (accessed 5/31/2018).
16. Manos D. 5 Ways to Avoid Health Data Breaches. Healthcare IT News. February 19, 2014. Available at: ***healthcareitnews.com/news/5-ways-avoid-health-data-breaches*** (accessed 5/31/2018).
17. Office of the National Coordinator for Health Information Technology (ONC). Guide to Privacy and Security of Electronic Health Information. Chapter 4. Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity. Available at: ***healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-4.pdf*** (accessed 5/31/2018).
18. Cornell Law School, Legal Information Institute. U.S. Code of Federal Regulations. 45 C.F.R. §164.304. - Definitions. Available at: ***law.cornell.edu/cfr/text/45/164.304*** (accessed 5/31/2018)
19. California Medical Association. CMA Legal Counsel, Document #4006, Security Breach of Health Information, January 2015.
20. Kam R. How to Protect Patient Information—and What to Do if It Gets Lost or Stolen. Psychiatric Times. November 21, 2015. Available at: ***psychiatrictimes.com/bipolar-disorder/how-protect-patient-information%E2%80%94and-what-do-if-it-gets-lost-or-stolen#sthash.IF9JUnJN.dpuf*** (accessed 5/31/2018).

CLAIMS Rx

CME ACTIVITY

ACCME ACCREDITED WITH COMMENDATION

HIPAA Data Breach Prevention and Management

Cases One & Two | PHI on Stolen Computers

Case Three | Comprised Flash Drive Data

Case Four | Compromised Email

Case Five | Employee Malicious Data Breach

MyNORCAL® CME APP

Earn CME credit for this *Claims Rx* article

- Read the *Claims Rx* article
- Open the MyNORCAL App using your existing MyACCOUNT credentials*
- Take a short quiz using the simple intuitive mobile interface
- Print or email your CME certificate or transcript

DOWNLOAD YOUR **FREE APP** NOW!

*Search '**MyNORCAL**' in the App Store or Google Play*

Download on the App Store

ANDROID APP ON Google play

**Contact NORCAL Customer Service at 844.4NORCAL to obtain your MyACCOUNT credentials*

NORCAL GROUP® 844.4NORCAL | *norcal-group.com*

NORCAL GROUP®

844.466.7225 | norcal-group.com

FOR ADDITIONAL CONTENT AND INFORMATION:

norcal-group.com/pandemic

Our Risk Management team is committed to assisting you:

 Monday-Friday from 8am – 8pm ET  855.882.3412  risksolutions@norcal-group.com